ACTA ARITHMETICA
143.3 (2010)

Arcs with no more than two integer points on conics

by

D. S. Ramana (Allahabad)

1. Introduction. The present article is set against the backdrop of the problem of studying gaps between integer points on affine conics as considered, for example, in [CJ]. The best result known on this problem, which is Theorem 1.4 of Cilleruelo and Jiménez-Urroz [CJ], tells us that when m is an integer ≥ 2, there are no more than m integer points on any arc of length $\ll_{a,d} |R|^{s(m)}$ on the conic $aX^2 + dY^2 = R$, where a, d and R are non-zero integers, and $s(m) = 1/4 - 1/(8[m/2] + 4)$. It appears to be a difficult problem to improve upon this result, although it is believed to be far from presenting the correct picture at least when the conic in question is a circle and $m \geq 4$ (see [CG], the penultimate paragraph on page 1237 and Conjecture 1 on page 1238). It is, however, known that when the conic is a circle or a rectangular hyperbola, that is, when $a = \pm d$, and $m = 2$ or 3 the dependence on R given by this result is optimal. When the conic is a circle, this follows from the much more detailed conclusions of Cilleruelo [C] when $m = 2$ and those of the recent work [CG] of Cilleruelo and Granville in the substantially more difficult case when $m = 3$. According to Section 10 of [CG], the case of the rectangular hyperbola is the subject of a forthcoming article by the same authors.

In this article we shall be concerned exclusively with the case $m = 2$ of the results reviewed above. More precisely, in Cilleruelo [C] it is shown that for any integer $R \geq 0$ an arc of length $2(4R)^{1/6}$ on the circle $X^2 + Y^2 = R$ contains no more than two integer points and, further, that for any $\epsilon > 0$ there are infinitely many integers $R \geq 0$ such that on the circle $X^2 + Y^2 = R$ there is an arc of length $\leq 2(4R)^{1/6} + \epsilon$ containing three integer points. Analogous conclusions for the rectangular hyperbola are stated on page 1236 of [CG]. Our principal purpose here is to take up the general case of conics given by $aX^2 + dY^2 = R$, where R, a and d are any non-zero integers. Clearly, we may assume that a and d are coprime. Our main results are then Theorems 1.1 and 1.2 below.

2010 *Mathematics Subject Classification*: Primary 11P21; Secondary 11L03.
Key words and phrases: integer points, conics, Cayley–Menger determinants.

DOI: 10.4064/aa143-3-1

For any integer $n \neq 0$, let $v_2(n)$ denote the largest integer k such that 2^k divides n. When $v_2(ad)$ is either 1 or 2, we set $m_{ad} = 4$, and when $v_2(ad)$ is either 0 or ≥ 3, we set $m_{ad} = 2$. In other words, $m_{ad} = 4$ when ad is congruent to 2, 4 or 6 modulo 8, and $m_{ad} = 2$ otherwise.

THEOREM 1.1. *Let a, d and R be non-zero integers and suppose that a and d are coprime. Then there are no more than two integer points on any arc of length*

$$\leq 2\left(\frac{|ad|m_{ad}^2|R|}{\sup(|a|,|d|)^3}\right)^{1/6}$$

on the conic $aX^2 + dY^2 = R$.

The conclusion of Theorem 1.1 is seen to be the best possible by means of the following theorem, which is stated in the pattern of Theorem 1.3 of [CG]. In Theorem 1.2 and thereafter we shall say that an arc of a conic *joins* a set of points in the plane if this arc contains this set of points and is the *shortest* of such arcs on the conic.

THEOREM 1.2. *Let a and d be non-zero coprime integers and let $\mathcal{A}$ be the set of real numbers C for which there is an integer R such that on the conic $aX^2+dY^2 = R$ there is an arc of length $2C\big(\frac{|ad|m_{ad}^2|R|}{\sup(|a|,|d|)^3}\big)^{1/6}$ that joins a set of three integer points. Then $\mathcal{A}$ is a dense subset of the interval $[1, +\infty)$.*

We prove Theorems 1.1 and 1.2 in Sections 3 and 4 respectively. We shall presently outline our proofs, which develop on the attractive proofs of Theorems 1.2 and 1.3 on page 1217 of [CG], where Cilleruelo and Granville revisit and refine the results of [C].

Let us call an ordered triple $\tau = (p_1, p_2, p_3)$ of non-collinear points p_i with coordinates (x_i, y_i) in the real plane a *triangle* and call the points p_i the *points of the triangle* τ. We write $\Delta(\tau)$ to denote the determinant whose ith row is $(x_i, y_i, 1)$ for $1 \leq i \leq 3$. Thus $|\Delta(\tau)|$ is twice the area of the Euclidean triangle with vertices p_i. We call $\Delta(\tau)$ the *determinant* of τ. When the p_i all have integer coordinates we say that τ is an *integer triangle*.

We now have the following simple but crucial remark, which we verify under Lemma 3.1. Given a and d, there is for any triangle $\tau = (p_1, p_2, p_3)$ a unique point $p(\tau) = (x(\tau), y(\tau))$ and a unique real number $R(\tau)$ such that the points p_1, p_2 and p_3 all lie on the conic

$$a(X - x(\tau))^2 + d(Y - y(\tau))^2 = R(\tau). \tag{1.1}$$

We call $p(\tau)$ the *centre of the triangle τ relative to* (a, d). Thus, given a and d, if $\tau = (p_1, p_2, p_3)$ is an integer triangle whose centre $p(\tau)$ relative to (a, d) is also an integer point, then $p_1 - p(\tau), p_2 - p(\tau)$ and $p_3 - p(\tau)$ are all integer points on $aX^2 + dY^2 = R(\tau)$. We shall repeatedly use this conclusion as our path to obtaining sets of three integer points all lying on $aX^2 + dY^2 = R$,

for some R. We refer to the triangle $(p_1 - p(\tau), p_2 - p(\tau), p_3 - p(\tau))$ as the triangle obtained by *translating* τ *by its centre relative to* (a, d).

Let us now summarize the proof of Theorem 1.1. Suppose that the points p_i of a triangle $\tau = (p_1, p_2, p_3)$ all lie on a circle of radius r. We then have the classical formula $\prod_{1 \le i < j \le 3} \|p_i - p_j\| = 2\Delta(\tau)r$, where $\| \ \|$ is the usual norm on $\mathbb{R}^2$, and on which the proof of Theorem 1.2 in [CG] is based. We begin by reviewing a generalisation of this formula given by Proposition 2.1. With the aid of the conclusion of the preceding paragraph and an analysis of $\Delta(\tau)$ modulo 2 we then show that, for a and d as in Theorem 1.1, m_{ad} is the infimum of $|\Delta(\tau)|$ taken over all integer triangles τ for which there is an $R(\tau)$ such that the points of τ all lie on $aX^2 + dY^2 = R(\tau)$. This together with an application of Proposition 2.1 gives Theorem 1.1.

It will be intuitively clear from the proof of Theorem 1.1 that, for sufficiently large R, an arc on $aX^2 + dY^2 = R$ joining the points of an integer triangle with determinant m_{ad} and whose points all "nearly" lie on a line parallel to a coordinate direction should show Theorem 1.1 to be optimal. For this reason, the proof of Theorem 1.2 reduces to producing, for infinitely many integers R, such "thin" triangles with points all lying on $aX^2 + dY^2 = R$. We obtain such triangles by translating, by their centres, triangles in the orbit of a suitably chosen integer triangle with determinant m_{ad} under the action of the principal congruence subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$, where $N = 2adm_{ad}$. Here we let $\mathrm{SL}_2(\mathbb{Z})$ act on the set of triangles by the natural extension of its action on the points of the plane as a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Theorems 1.1 and 1.2 evidently imply an optimal lower bound for the diameter of any set of three integer points on a given conic of the form $aX^2 + dY^2 = R$. In Section 5, which is the final section of this article, we consider, more generally, the case of $n + 1$ integer points on quadrics of the form $a_1X_1^2 + \cdots + a_nX_n^2 = R$, where the a_i and R are integers, and n is an integer ≥ 2. Our results in this case are Propositions 5.1 and 5.2, which, though less precise, are analogues of Theorems 1.1 and 1.2 for these quadrics and are obtained by analogous arguments.

Throughout this article, when A is a matrix, A^t shall mean the transpose of A.

2. A classical formula. Special cases of the formula given by Proposition 2.1 below may be found in pages 238 to 242 of [B], in connection with the Cayley–Menger determinant, and in Ex. 10, page 26 of [S], from which sources its proof, provided below for completeness, may be easily deduced.

Let n be an integer ≥ 2 and suppose that a_i, c_i, $1 \le i \le n$, and R are all real numbers. Let $\tau = (p_1, \ldots, p_{n+1})$, with $p_i = (x_{1i}, \ldots, x_{ni})$, be a tuple

of $n+1$ points in $\mathbb{R}^n$, all lying on

$$a_1(X_1-c_1)^2+\cdots+a_n(X_n-c_n)^2=R. \tag{2.1}$$

Let $\Delta(\tau)$ be the determinant of the the square matrix of order $n+1$ whose ith row is $(x_{1i},\dots,x_{ni},1)$. Further, let $\mathrm{P}(\tau)$ be the square matrix of order $n+1$ whose (i,j)th entry is $a_1(x_{1i}-x_{1j})^2+\cdots+a_n(x_{ni}-x_{nj})^2$.

PROPOSITION 2.1. *With notation as above we have the relation*

$$\det(\mathrm{P}(\tau))=(-1)^n\,2^{n+1}\Big(\prod_{1\le i\le n}a_i\Big)\,\Delta(\tau)^2R. \tag{2.2}$$

Proof. Since both sides of (2.2) are invariant on replacing the p_i with p_i-c, where $c=(c_1,\dots,c_n)$, we assume that $c_i=0$ for each i. Let α_i, for $1\le i\le n$, and β be complex numbers satisfying the relations $\alpha_i^2=a_i$ and $\beta^2=R$. Let $\mathrm{M}_+(\tau)$ be the square matrix of order $n+1$ whose ith row is $(\alpha_1x_{1i},\dots,\alpha_nx_{ni},\beta)$ and $\mathrm{M}_-(\tau)$ be the square matrix of order $n+1$ whose ith row is $(\alpha_1x_{1i},\dots,\alpha_nx_{ni},-\beta)$. Since the points p_i lie on (2.1), and since the c_i are all 0, we have the identity

$$\sum_{1\le k\le n}a_k(x_{ki}-x_{kj})^2=-2\Big(-R+\sum_{1\le k\le n}a_kx_{ki}x_{kj}\Big)$$

for any (i,j) with $1\le i\le j\le n+1$. This identity implies the relation of matrices $\mathrm{P}(\tau)=-2\mathrm{M}_-(\tau)\mathrm{M}_+(\tau)^t$, from which (2.2) results on passing to determinants and noting that $\det(\mathrm{M}_\pm(\tau))=\pm\Delta(\tau)\beta\prod_{1\le i\le n}\alpha_i$. ∎

3. The bound for conics. When $\alpha=(\alpha_1,\alpha_2,\alpha_3)$, $\beta=(\beta_1,\beta_2,\beta_3)$ are ordered triples of real numbers and i and j integers ≥ 1, we set

$$\Delta_{ij}(\alpha,\beta)=\det\begin{pmatrix}\alpha_1^i&\beta_1^j&1\\ \alpha_2^i&\beta_2^j&1\\ \alpha_3^i&\beta_3^j&1\end{pmatrix}. \tag{3.1}$$

LEMMA 3.1. *Let a and d be real numbers $\neq 0$ and $\tau=(p_1,p_2,p_3)$ with $p_i=(x_i,y_i)$ be a triangle. Then there is a unique $(x(\tau),y(\tau),R(\tau))$ in $\mathbb{R}^3$ such that the points p_i all lie on the conic*

$$a(X-x(\tau))^2+d(Y-y(\tau))^2=R(\tau). \tag{3.2}$$

If x and y denote (x_1,x_2,x_3) and (y_1,y_2,y_3) respectively then

$$2a\Delta(\tau)x(\tau)=a\Delta_{21}(x,y)+d\Delta_{21}(y,y), \tag{3.3}$$

$$2d\Delta(\tau)y(\tau)=a\Delta_{12}(x,x)+d\Delta_{12}(x,y). \tag{3.4}$$

Proof. Since the p_i are not collinear, $\Delta(\tau) \neq 0$. Thus there exists a unique $(x(\tau), y(\tau), z(\tau))$ in $\mathbb{R}^3$ satisfying the matrix relation

$$\begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} \begin{pmatrix} 2ax(\tau) \\ 2dy(\tau) \\ z(\tau) \end{pmatrix} = \begin{pmatrix} ax_1^2 + dy_1^2 \\ ax_2^2 + dy_2^2 \\ ax_3^2 + dy_3^2 \end{pmatrix}. \tag{3.5}$$

On setting $R(\tau) = z(\tau) + ax(\tau)^2 + dy(\tau)^2$, we easily deduce from (3.5) that the p_i all lie on the conic (3.2) and that $(x(\tau), y(\tau), R(\tau))$ is uniquely determined by (a, d) and τ. Finally, Cramer's rule applied to (3.5) gives (3.3) and (3.4). ∎

The point $p(\tau) = (x(\tau), y(\tau))$ is what has been called the *centre of a triangle τ relative to* (a, d) in Section 1. For the sake of brevity, we sometimes omit mentioning (a, d) when referring to the centre of a triangle τ relative to (a, d). We shall denote the conic (3.2) by $\mathcal{C}_{ad}(\tau)$.

LEMMA 3.2. *For any non-zero coprime integers a and d there is an integer triangle whose centre relative to (a, d) is an integer point and whose determinant is m_{ad}.*

Proof. Let b and c be any integers such that $ab - cd = 1$. The lemma is a consequence of the definition of m_{ad} and the following assertions, which we shall verify presently.

(i) $((2b, 2c), (d, a), (0, 0))$ is an integer triangle with determinant 2. When $v_2(ad) = 0$, the centre of this triangle relative to (a, d) is an integer point.

(ii) $((1, 1), (-1, 1), (1, -1))$ is an integer triangle with determinant 4. For any a and d and, in particular, when $v_2(ad) = 1$ or 2, the centre of this triangle relative to (a, d) is $(0, 0)$.

(iii) $((2b, 4c), (d/2, a), (0, 0))$ is a triangle with determinant 2. When $v_2(ad) \geq 3$ and a is odd, this triangle is an integer triangle whose centre relative to (a, d) is an integer point.

(iv) $((4b, 2c), (d, a/2), (0, 0))$ is a triangle with determinant 2. When $v_2(ad) \geq 3$ and a is even, this triangle is an integer triangle whose centre relative to (a, d) is an integer point.

All other assertions above being evident, we are reduced to verifying that the centres of the triangles given in (i), (iii) and (iv) are indeed integer points. Let us consider the case of the triangle $\tau = ((2b, 2c), (d, a), (0, 0))$ in (i). Since $\Delta(\tau) = 2$, the formula (3.3) gives

$$4ax(\tau) = a \det \begin{pmatrix} 4b^2 & 2c & 1 \\ d^2 & a & 1 \\ 0 & 0 & 1 \end{pmatrix} + d \det \begin{pmatrix} 4c^2 & 2c & 1 \\ a^2 & a & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.6}$$

On expanding the determinants in (3.6) by their last rows and dividing throughout by $2a$ we get

$$2x(\tau) = \det\begin{pmatrix} 2b^2 & c \\ d^2 & a \end{pmatrix} + d\det\begin{pmatrix} 2c^2 & c \\ a & 1 \end{pmatrix} \equiv 2\det\begin{pmatrix} 0 & c \\ 1 & 1 \end{pmatrix} \equiv 0 \bmod 2, \tag{3.7}$$

since a and d are both odd. Thus $x(\tau)$ is an integer. The formula (3.4) gives

$$4dy(\tau) = a\det\begin{pmatrix} 2b & 4b^2 & 1 \\ d & d^2 & 1 \\ 0 & 0 & 1 \end{pmatrix} + d\det\begin{pmatrix} 2b & 4c^2 & 1 \\ d & a^2 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.8}$$

On expanding the determinants in (3.8) by their last rows and dividing throughout by $2d$ we get

$$2y(\tau) = a\det\begin{pmatrix} b & 2b^2 \\ 1 & d \end{pmatrix} + \det\begin{pmatrix} b & 2c^2 \\ d & a^2 \end{pmatrix} \equiv 2\det\begin{pmatrix} b & 0 \\ 1 & 1 \end{pmatrix} \equiv 0 \bmod 2, \tag{3.9}$$

since a and d are odd. Thus $y(\tau)$ is an integer.

Let us now consider the triangle $\tau = ((2b, 4c), (d/2, a), (0, 0))$ in (iii). When $v_2(ad) \geq 3$ and a is odd, we have $v_2(d) \geq 3$, since a and d are coprime. Thus τ is an integer triangle. Further, from the formula (3.3) we have

$$4ax(\tau) = a\det\begin{pmatrix} 4b^2 & 4c & 1 \\ d^2/4 & a & 1 \\ 0 & 0 & 1 \end{pmatrix} + d\det\begin{pmatrix} 16c^2 & 4c & 1 \\ a^2 & a & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.10}$$

On expanding the determinants in (3.10) by their last rows and dividing throughout by $4a$ we get

$$x(\tau) = \det\begin{pmatrix} b^2 & c \\ d^2/4 & a \end{pmatrix} + d\det\begin{pmatrix} 4c^2 & c \\ a & 1 \end{pmatrix}, \tag{3.11}$$

so that $x(\tau)$ is an integer. Using the formula (3.4) for $y(\tau)$ we get

$$4dy(\tau) = a\det\begin{pmatrix} 2b & 4b^2 & 1 \\ d/2 & d^2/4 & 1 \\ 0 & 0 & 1 \end{pmatrix} + d\det\begin{pmatrix} 2b & 16c^2 & 1 \\ d/2 & a^2 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.12}$$

On expanding the determinants in (3.12) by their last rows and dividing throughout by d we get

$$4y(\tau) = a\det\begin{pmatrix} b & 2b^2 \\ 1 & d/2 \end{pmatrix} + \det\begin{pmatrix} 2b & 16c^2 \\ d/2 & a^2 \end{pmatrix} \equiv 2ab(a-b) \bmod 4, \tag{3.13}$$

since $d/2$ is divisible by 4. For any integers a and b the product $2ab(a-b)$ is divisible by 4. Thus $y(\tau)$ is an integer. The case of the triangle in (iv) being similar to that in (iii), we leave this case to the reader. ∎

PROPOSITION 3.3. *When a and d are non-zero coprime integers, the infimum of $|\Delta(\tau)|$ taken over all integer triangles τ which have an integer point for their centre relative to (a,d) is m_{ad}.*

Proof. On account of Lemma 3.2, we are reduced to showing that $|\Delta(\tau)| \geq m_{ad}$ for any integer triangle τ whose centre relative to (a,d) is an integer point. Since $\Delta(\tau)$ is then a non-zero integer, it suffices to verify that

$$2^{v_2(\Delta(\tau))} \geq m_{ad}\,. \tag{3.14}$$

Translating the points of τ by the centre of τ we assume that the points of τ lie on the conic $aX^2 + dY^2 = R$, for some integer R. Further, by symmetry, we assume that a is odd so that $v_2(ad) = v_2(d)$.

All integer points (x,y) on $aX^2+dY^2 = R$ satisfy $ax+dy = R$ modulo 2. Since a is odd, it follows that the integer points on $aX^2 + dY^2 = R$ reduce modulo 2 to no more than two points. Therefore at least two of the three rows of $\Delta(\tau)$ are the same modulo 2 and hence $v_2(\Delta(\tau)) \geq 1$. In particular, this implies (3.14) when $v_2(ad) = v_2(d) = 0$ or ≥ 3.

Suppose that either (i) $v_2(ad) = v_2(d) = 1$ or (ii) R is odd and $v_2(ad) = v_2(d) = 2$. We will obtain (3.14) in these cases by verifying that all integer points of τ reduce to the same point modulo 2 so that all rows of $\Delta(\tau)$ are the same modulo 2 and $v_2(\Delta(\tau)) \geq 2$. To this end, let (x_i, y_i) be the points of τ.

When (i) holds we have $ax_i^2 + dy_i^2 = R$ with d even and a odd so that each x_i is the same as R modulo 2. Thus $x_i \equiv x_j \bmod 2$ and hence $x_i^2 - x_j^2 \equiv 0 \bmod 4$, for any i and j. Since we have $a(x_i^2 - x_j^2) = -d(y_i^2 - y_j^2)$ with $v_2(a) = 0$ and $v_2(d) = 1$, this implies that $y_i^2 - y_j^2 \equiv 0 \bmod 2$ for any i and j. Consequently, (x_i, y_i) and (x_j, y_j) are the same modulo 2 for any i and j when (i) holds.

When (ii) holds we have $ax_i^2 + dy_i^2 = R$ with R odd, d even and a odd. Thus each x_i is odd and hence $x_i^2 - x_j^2 \equiv 0 \bmod 8$ for any i and j. Since $a(x_i^2 - x_j^2) = -d(y_i^2 - y_j^2)$ with $v_2(a) = 0$ and $v_2(d) = 2$, this implies that $y_i^2 - y_j^2 \equiv 0 \bmod 2$ for any i and j. Consequently, (x_i, y_i) and (x_j, y_j) are the same modulo 2 for any i and j when (ii) holds.

Suppose now that R is even and $v_2(ad) = v_2(d) = 2$. Then each x_i is even and the triangle τ' whose points have the coordinates $(x_i/2, y_i)$ is an integer triangle lying on $aX^2 + (d/4)Y^2 = R/4$. Since a and $d/4$ are non-zero coprime integers, $v_2(\Delta(\tau')) \geq 1$. Since $\Delta(\tau) = 2\Delta(\tau')$ we conclude that $v_2(\Delta(\tau)) \geq 2$, from which (3.14) follows in this case as well. ∎

Proof of Theorem 1.1. Let $p_i = (x_i, y_i)$, $1 \le i \le 3$, be three integer points on $aX^2 + dY^2 = R$, all lying on an arc $\mathcal{A}$ of length l. We shall verify that $l > 2\big(\frac{|ad|m_{ad}^2|R|}{\sup(|a|,|d|)^3}\big)^{1/6}$. Let τ denote the triangle (p_1, p_2, p_3).

Applying Proposition 2.1 to the ordered triple τ and $aX^2+dY^2 = R$, and noting that, in this case, $\det(\mathrm{P}(\tau)) = 2\prod_{1\le i<j\le 3}(a(x_i - x_j)^2 + d(y_i - y_j)^2)$, we obtain

$$\prod_{1\le i<j\le 3} (a(x_i - x_j)^2 + d(y_i - y_j)^2) = 4ad\Delta(\tau)^2 R. \tag{3.15}$$

For each (i, j) with $1 \le i < j \le 3$, let l_{ij} denote the length of the part of $\mathcal{A}$ that joins p_i and p_j. Then $\sup(|a|, |d|)l_{ij}^2 > |a(x_i - x_j)^2 + d(y_i - y_j)^2|$ for each such (i, j). On taking absolute values of both sides of (3.15) and using Proposition 3.3 we then have

$$\sup(|a|, |d|)^3(l_{12}l_{23}l_{13})^2 > 4|ad|\,|\Delta(\tau)|^2|R| \ge 4|ad|m_{ad}^2|R|. \tag{3.16}$$

We may assume that p_2 lies on the part of $\mathcal{A}$ that joins p_1 and p_3. We then have $l_{12} + l_{23} = l_{13} \le l$ and consequently $l_{12}l_{23} \le l^2/4$ and $l_{12}l_{23}l_{13} \le l^3/4$. On combining this remark with (3.16) and rearranging terms we obtain the required lower bound for l.

4. Optimality of the bound for conics. Throughout this section, a and d shall be given non-zero coprime integers. When τ is a triangle we write $\mathrm{dia}(\tau)$ to denote the largest of the distances between the points of τ.

Let $\mathcal{T}_{ad}$ be the set of integer triangles τ whose centres relative to (a, d) are integer points and for which on the conic $\mathcal{C}_{ab}(\tau)$ defined by (3.2) there exists an arc that joins the points of τ. When a and d are of the same sign, $\mathcal{C}_{ad}(\tau)$ is an ellipse and there exists such an arc on $\mathcal{C}_{ad}(\tau)$ for all triangles τ. This may not, however, be the case for all triangles τ when a and d are of opposite signs, that is, when $\mathcal{C}_{ad}(\tau)$ is a hyperbola, for then the points of τ may not all lie on the same branch. Since the distance between the two branches of a hyperbola $a(X - k)^2 + d(Y - l)^2 = R$, where (k, l) is a point in the plane, is at least $2(|R|/\sup(|a|, |d|))^{1/2}$, it suffices to verify that $\mathrm{dia}(\tau) < 2(|R(\tau)|/\sup(|a|, |d|))^{1/2}$ in order to conclude that a triangle τ lies in $\mathcal{T}_{ad}$, for any a and d.

We borrow notation from Cilleruelo and Granville [CG] and write $\mathrm{Arc}(\tau)$, for each τ in $\mathcal{T}_{ad}$, to denote the length of the arc on $\mathcal{C}_{ad}(\tau)$ that joins the points of τ. We shall presently verify the following theorem.

THEOREM 4.1. *Let a and d be non-zero coprime integers. The image of the map*

$$\tau \mapsto \frac{\mathrm{Arc}(\tau)}{2\big(\frac{|ad|m_{ad}^2|R(\tau)|}{(\sup(|a|,|d|)^3}\big)^{1/6}} \tag{4.1}$$

from $\mathcal{T}_{ad}$ to the real line is a dense subset of the interval $[1, +\infty)$.

Theorem 1.2 follows immediately from Theorem 4.1 on translating the triangles τ in $\mathcal{T}_{ad}$ by their centres relative to (a, d).

We extend the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$ on the points of the plane as a subgroup of $\mathrm{GL}_2(\mathbb{R})$ to the set of all triangles by setting $g(\tau) = (g(p_1), g(p_2), g(p_3))$ for any triangle $\tau = (p_1, p_2, p_3)$ and g in $\mathrm{SL}_2(\mathbb{Z})$. We prove Theorem 4.1 at the end of this section with the aid of the following lemmas. We recall that, for any integer N, $\Gamma(N)$ is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ all of whose elements reduce to the identity matrix modulo N.

LEMMA 4.2. *Let τ be an integer triangle whose centre is an integer point and let τ' be a triangle in the orbit of τ under $\Gamma(2ad\Delta(\tau))$. Then $\Delta(\tau') = \Delta(\tau)$ and the centre of τ' is an integer point.*

Proof. Let g in $\Gamma(2ad\Delta(\tau))$ be such that $\tau' = g(\tau)$. Since $\det(g) = 1$ we have $\Delta(\tau') = \det(g)\Delta(\tau) = \Delta(\tau)$. Suppose $\tau = (p_1, p_2, p_3)$. Since g reduces to the identity matrix modulo $2ad\Delta(\tau)$, the point $g(p_i)$ is the same as p_i modulo $2ad\Delta(\tau)$ for each i. The formulae (3.3) and (3.4) then imply that the centre of τ' is an integer point. ∎

LEMMA 4.3. *Let $\tau = (p_1, p_2, p_3)$ with $p_i = (x_i, y_i)$ be a triangle that satisfies the conditions $x_1 > x_2$, $x_1 > x_3$ and $\Delta(\tau) > 0$. Then*

$$-\frac{y_1 - y_2}{x_1 - x_2} > -\frac{y_1 - y_3}{x_1 - x_3}.$$

If I_τ is the non-empty open interval $\left(-\frac{y_1-y_3}{x_1-x_3}, -\frac{y_1-y_2}{x_1-x_2}\right)$ then for all t in I_τ we have

$$tx_2 + y_2 > tx_1 + y_1 > tx_3 + y_3. \tag{4.2}$$

Moreover, if $f_\tau(t)$ is the rational function defined by

$$f_\tau(t) = \frac{(t(x_2 - x_3) + (y_2 - y_3))^2}{4(t(x_2 - x_1) + (y_2 - y_1))(t(x_1 - x_3) + (y_1 - y_3))}, \tag{4.3}$$

then f_τ maps I_τ continuously on $[1, +\infty)$.

Proof. We have $\Delta(\tau) = (x_1 - x_2)(y_1 - y_3) - (x_1 - x_3)(y_1 - y_2)$. It then follows from the hypothesis on τ that $-\frac{y_1-y_2}{x_1-x_2} > -\frac{y_1-y_3}{x_1-x_3}$. All other assertions of the lemma being evident, it remains to verify that the image of I_τ under f_τ is $[1, +\infty)$. To see this, we note using (4.3) that

$$f_\tau(t) - 1 = \frac{(t(x_2 - x_1 + x_3 - x_1) + (y_2 - y_1 + y_3 - y_1))^2}{4(t(x_2 - x_1) + (y_2 - y_1))(t(x_1 - x_3) + (y_1 - y_3))}, \tag{4.4}$$

from which and (4.2) it follows that $f_\tau(t) \geq 1$ for all t in I_τ. Moreover, $f_\tau(t) = 1$ when $t = \frac{-(y_1-y_2)-(y_1-y_3)}{(x_1-x_2)+(x_1-x_3)}$, and this point lies in I_τ. We conclude by noting that $f_\tau(t)$ tends to $+\infty$ as t tends to either end point of I_τ. ∎

From this point on we will assume, as we may without loss of generality, that $\sup(|a|,|d|) = |a|$. Further, set $N = 2adm_{ad}$ and, for each integer m,

$$S_m = \begin{pmatrix} 1 & Nm \\ 0 & 1 \end{pmatrix}, \tag{4.5}$$

which is an element of $\Gamma(N)$. For any triangle $\tau = (p_1, p_2, p_3)$ and an integer m we write τ^m to denote the triangle $S_m(\tau)$, and denote the points $S_m(p_i)$ of τ^m by p_i^m. By Lemma 4.2, $\Delta(\tau^m) = \Delta(\tau)$ and τ^m is an integer triangle whose centre is an integer point, if this is so for τ. If (x_i, y_i) are the coordinates of p_i and, for each integer m, (x_i^m, y_i^m) are the coordinates of p_i^m, we have

$$x_i^m = Nmy_i + x_i \quad \text{and} \quad y_i^m = y_i \quad \text{for each } i. \tag{4.6}$$

LEMMA 4.4. *Let τ be an integer triangle with $\Delta(\tau) = m_{ad}$ and whose centre relative to (a,d) is an integer point. Suppose further that the points $p_i = (x_i, y_i)$, $1 \le i \le 3$, of τ satisfy the condition $y_2 > y_1 > y_3$. Then τ^m is in $\mathcal{T}_{ab}$ for all sufficiently large integers m, and*

$$\lim_{m\to+\infty} \frac{\mathrm{Arc}(\tau^m)}{2\big(\frac{|ad|m_{ad}^2|R(\tau^m)|}{|a|^3}\big)^{1/6}} = \lim_{m\to+\infty} \frac{\mathrm{dia}(\tau^m)}{2\big(\frac{|ad|m_{ad}^2|R(\tau^m)|}{|a|^3}\big)^{1/6}} = \left(\frac{(y_2-y_3)^2}{4(y_2-y_1)(y_1-y_3)}\right)^{1/3}. \tag{4.7}$$

Proof. From (4.6) we have for any (i,j), as $m \to +\infty$,

$$|(a(x_i^m - x_j^m)^2 + d(y_i^m - y_j^m)^2)| \sim |a|\,|N|^2 m^2 |y_i - y_j|^2.$$

Since $y_2 > y_1 > y_3$, we further have $\mathrm{dia}(\tau^m) \sim |N|m(y_2 - y_3)$ as $m \to +\infty$. These remarks together with (3.15) give the second equality in (4.7).

Since $\mathrm{dia}(\tau^m) \to +\infty$ as $m \to +\infty$, the second equality in (4.7) implies that $|R(\tau^m)| \to +\infty$ as $m \to +\infty$ and $\mathrm{dia}(\tau^m) \ll_{a,d} |R(\tau^m)|^{1/6}$. Consequently, τ^m is in $\mathcal{T}_{ad}$ for all sufficiently large m and $\mathrm{dia}(\tau^m)/|R(\tau^m)|^{1/2} \to 0$ as $m \to +\infty$. Thus $\mathrm{Arc}(\tau^m)/\mathrm{dia}(\tau^m) \to 1$ as $m \to +\infty$, so that the first equality in (4.7) holds as well. ∎

Proof of Theorem 4.1. By Lemma 3.2 there is an integer triangle τ with determinant m_{ad} and whose centre relative to (a,d) is an integer point. Replacing τ with τ^m, for a sufficiently large m, and then changing the ordering on the set of points of τ if necessary, we may assume that τ satisfies the conditions of Lemma 4.3. Let $\mathcal{E}$ be the set of rational numbers in the interval I_τ which, in their reduced form, may be expressed as r/s, with r and s coprime, $s > 0$ and $r \equiv 0 \bmod N$, $s \equiv 1 \bmod N$.

If t is in $\mathcal{E}$ and r/s is its reduced form, then there exist integers p, q such that

$$T_t = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is in $\Gamma(N)$. Let τ_t be the triangle $T_t(\tau)$. By Lemma 4.2, τ_t is an integer triangle with an integer point as centre and determinant m_{ad}. Since t is in I_τ, (4.2) implies that τ_t satisfies the conditions of Lemma 4.4. In particular, on applying (4.7) to τ_t, we see that $f_\tau(t)^{1/3}$ is a limit point of the image of the map (4.1). Thus the closure of that image contains the closure of the image of $\mathcal{E}$ under $f_\tau^{1/3}$, which is $[1, +\infty)$ by Lemma 4.3, as $\mathcal{E}$ is dense in I_τ. Since, by Theorem 1.1, the image of the map (4.1) is contained in $[1, +\infty)$, we obtain Theorem 4.1.

5. An analogue in higher dimensions. Throughout this section we use the notation introduced in Section 2. Further, for positive integers n and k and any tuple $\tau = (p_1, \dots, p_k)$ of points in $\mathbb{R}^n$, write $\mathrm{dia}(\tau)$ to denote $\sup_{1\le i\le j\le k} \|p_i - p_j\|$, where $\| \ \|$ denotes the usual norm on $\mathbb{R}^n$.

PROPOSITION 5.1. *Let n be an integer ≥ 2 and suppose that a_i, $1 \le i \le n$, and R are non-zero integers. Let $\tau = (p_1, \dots, p_{n+1})$ be a tuple of $n+1$ integer points in $\mathbb{R}^n$, all lying on*

$$a_1 X_1^2 + \cdots + a_n X_n^2 = R. \tag{5.1}$$

When $\Delta(\tau) \ne 0$ we have

$$\mathrm{dia}(\tau) \ge \sqrt{2}\left(\frac{\prod_{1\le i\le n} |a_i|\,|R|}{(n+1)!(\sup_{1\le i\le n} |a_i|)^{n+1}} \right)^{1/(2(n+1))}. \tag{5.2}$$

Proof. On expanding $\det(\mathrm{P}(\tau))$ by any row and applying the triangle inequality we have $|\det(\mathrm{P}(\tau))| \le (n+1)!(\sup_{1\le i\le n} |a_i|)^{n+1} \mathrm{dia}(\tau)^{2(n+1)}$. The proposition follows on combining this bound with the formula (2.2) and noting that $|\Delta(\tau)| \ge 1$, since $\Delta(\tau)$ is a non-zero integer. ∎

When $n = 2$, any tuple τ of $n+1$, that is, three distinct points lying on (5.1) satisfies the condition $\Delta(\tau) \ne 0$, so that this condition becomes superfluous in that case, as in Theorem 1.1. Plainly, this is not true when $n \ge 3$, since, for example, one can have four distinct coplanar points all lying on a given sphere in $\mathbb{R}^3$. The example due to R. Heath-Brown, cited by Cilleruelo and Granville in the final paragraph of Section 11 of [CG], then shows that it is possible to construct tuples τ of $n+1$ distinct integer points, all lying on a sphere in $\mathbb{R}^n$, which satisfy $\Delta(\tau) = 0$ and for which the lower bound for $\mathrm{dia}(\tau)$ given by Proposition 5.1 does not hold.

The following proposition, though much less precise than Theorem 1.2, shows, on the other hand, that when its hypotheses are satisfied the conclusion of Proposition 5.1 gives the best possible dependence on $|R|$.

PROPOSITION 5.2. *Let n be an integer ≥ 2 and a_i, $1 \leq i \leq n$, be non-zero integers. There is a real number $C > 0$ such that for infinitely many integers R there are tuples τ of $n+1$ integer points on $a_1X_1^2+\cdots+a_nX_n^2 = R$ satisfying $\Delta(\tau) \neq 0$ and $\mathrm{dia}(\tau) \leq C|R|^{1/(2(n+1))}$.*

We shall employ the following notation and lemma to verify this proposition, the principle being the same as that of the proof of Theorem 4.1. Let $\tau = (p_1, \ldots, p_{n+1})$ be a tuple of $n+1$ points $p_i = (x_{1i}, \ldots, x_{ni})$ in $\mathbb{R}^n$ satisfying $\Delta(\tau) \neq 0$. There is then a unique $(x_1(\tau), \ldots, x_n(\tau), z(\tau))$ in $\mathbb{R}^{n+1}$ satisfying the relation

$$\begin{pmatrix} x_{11} & \ldots & x_{n1} & 1 \\ \vdots & & \vdots & \vdots \\ x_{1n} & \ldots & x_{nn} & 1 \\ x_{1(n+1)} & \ldots & x_{n(n+1)} & 1 \end{pmatrix} \begin{pmatrix} 2a_1x_1(\tau) \\ \vdots \\ 2a_nx_n(\tau) \\ z(\tau) \end{pmatrix} = \begin{pmatrix} \mathcal{N}(p_1) \\ \vdots \\ \mathcal{N}(p_n) \\ \mathcal{N}(p_{n+1}) \end{pmatrix}, \tag{5.3}$$

where we have written $\mathcal{N}(p_i)$ for $a_1x_{1i}^2 + \cdots + a_nx_{ni}^2$, for each i. On setting $R(\tau) = z(\tau) + a_1x_1(\tau)^2 + \cdots + a_nx_n(\tau)^2$ we see from (5.3) that the points p_i all lie on

$$a_1(X_1 - x_1(\tau))^2 + \cdots + a_n(X_n - x_n(\tau))^2 = R(\tau).$$

We write $p(\tau)$ to denote the point $(x_1(\tau), \ldots, x_n(\tau))$ and call it the centre of τ relative to $(a_1, \ldots, a_n)$. Further, we set $\mathrm{D}(\tau)$ to be the determinant of order $n+1$ whose (i,j)th entry is $a_2(x_{2i} - x_{2j})^2 + \cdots + a_n(x_{ni} - x_{nj})^2$.

LEMMA 5.3. *There exists a tuple τ of $n+1$ integer points $p_1, \ldots, p_{n+1}$ whose centre relative to $(a_1, \ldots, a_n)$ is an integer point and such that $\Delta(\tau)$ and $\mathrm{D}(\tau)$ are distinct from 0.*

Proof. Let us first verify that there exists a tuple $\tau = (p_1, \ldots, p_{n+1})$ of $n+1$ points in $\mathbb{R}^n$ with each of the points p_i having rational coordinates and for which $\Delta(\tau)$, $\mathrm{D}(\tau)$ are $\neq 0$. By a familiar density argument, this reduces to verifying that the polynomials $\Delta(X_{11}, X_{21}, \ldots, X_{n(n+1)})$ and $\mathrm{D}(X_{11}, X_{21}, \ldots, X_{n(n+1)})$, obtained by replacing the coordinates x_{ij} of the points p_i in $\Delta(\tau)$ and $\mathrm{D}(\tau)$ with indeterminates X_{ij}, are distinct from the zero polynomial. This assertion being evident for $\Delta(X_{11}, X_{21}, \ldots, X_{n(n+1)})$, we take up the case of $\mathrm{D}(X_{11}, X_{21}, \ldots, X_{n(n+1)})$. For each i, $1 \leq i \leq n$, let α_i be a complex number satisfying $\alpha_i^2 = a_i$. Further, for each i, $1 \leq i \leq n+1$, let u_i denote the vector

$$(a_2X_{2i}^2 + \cdots + a_nX_{ni}^2, 1, \sqrt{-2}\,\alpha_2X_{2i}, \ldots, \sqrt{-2}\,\alpha_nX_{ni})$$

and let v_i denote the vector

$$(1, a_2X_{2i}^2 + \cdots + a_nX_{ni}^2, \sqrt{-2}\,\alpha_2X_{2i}, \ldots, \sqrt{-2}\,\alpha_nX_{ni}).$$

If U and V are respectively the matrices of order $n+1$ with ith rows u_i and v_i, it is easily seen that $\det(U)$ and $\det(V)$ are non-zero polynomials, since each a_i is non-zero. Moreover, $\det(U)\det(V) = \det(UV^t) = \mathrm{D}(X_{11}, X_{21}, \ldots, X_{n(n+1)})$. Thus, $\mathrm{D}(X_{11}, X_{21}, \ldots, X_{n(n+1)})$ is a non-zero polynomial. Finally, on multiplying all the coordinates of all the points of τ by a sufficiently large integer we obtain a tuple of $n+1$ integer points whose centre relative to $(a_1, \ldots, a_n)$ is also an integer point and which satisfies the conditions of the lemma. ∎

Proof of Proposition 5.2. Let $\tau = (p_1, \ldots, p_{n+1})$ be an $n+1$-tuple satisfying the conditions of Lemma 5.3, set $N = 2\prod_{1\le i\le n} a_i \Delta(\tau)$ and, for each integer m, let S_m be the upper triangular matrix of order n

$$\begin{pmatrix} 1 & Nm & 0 & \ldots & 0 \\ 0 & 1 & Nm & \ldots & 0 \\ \vdots & \ldots & 1 & Nm & \vdots \\ 0 & \ldots & 0 & 1 & Nm \\ 0 & \ldots & 0 & 0 & 1 \end{pmatrix}. \tag{5.4}$$

If, for each integer $m \ge 1$, τ^m is the tuple $(S_m(p_1), \ldots, S_m(p_{n+1}))$ then $\Delta(\tau^m) = \Delta(\tau)$ and, by Cramer's rule applied to (5.3), τ^m is a tuple of $n+1$ integer points whose centre relative to $(a_1, \ldots, a_n)$ is an integer point (cf. proof of Lemma 4.2). Also, it is easily seen that $\det(\mathrm{P}(\tau^m)) \sim (Nm)^{2(n+1)}\mathrm{D}(\tau)$ as $m \to +\infty$. Further, if $p_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ then let $q_i = (x_{i2}, \ldots, x_{in})$, for $1 \le i \le n+1$. If τ_1 is the tuple of $n+1$ points $q_1, \ldots, q_{n+1}$ in $\mathbb{R}^{n-1}$ then $\mathrm{dia}(\tau^m) \sim m|N|\mathrm{dia}(\tau_1)$ as $m \to +\infty$. It now follows from (2.2) that

$$\lim_{m\to+\infty} \frac{\mathrm{dia}(\tau^m)}{(2^{n+1}\prod_{1\le i\le n}|a_i|\,|R(\tau^m)|)^{1/(2(n+1))}} = \frac{\mathrm{dia}(\tau_1)}{|\mathrm{D}(\tau)|^{1/(2(n+1))}}. \tag{5.5}$$

Since $\Delta(\tau) \ne 0$ we have $\mathrm{dia}(\tau_1) \ne 0$. Therefore, $\mathrm{dia}(\tau^m) \to +\infty$ as $m \to +\infty$, and (5.5) implies that $|R(\tau^m)| \to +\infty$ as $m \to +\infty$. Thus the proposition follows on translating the tuples τ^m by their centres and taking (5.5) into account.

Acknowledgments. I wish to express my gratitude to Professor Joseph Oesterlé for providing me with an example (Example 2.1, page 357 of [R]) that led to this article. I am most thankful to Professor R. Balasubramanian and Professor Olivier Ramaré for their comments on this article. I am further indebted to Professor Ramaré for very kindly and generously hosting me on a visit supported by the IFIM programme to the University of Lille I, where work on this article was completed. I am grateful to the referee for providing me with a number of useful suggestions.

References

[B] M. Berger, *Geometry, I*, Springer, 1980.

[C] J. Cilleruelo, *Arcs containing no three lattice points*, Acta Arith. 59 (1991), 87–90.

[CG] J. Cilleruelo and A. Granville, *Close lattice points on circles*, Canad. J. Math. 61 (2009), 1214–1238.

[CJ] J. Cilleruelo and J. Jiménez-Urroz, *Divisors in a Dedekind domain*, Acta Arith. 85 (1998), 229–233.

[R] D. S. Ramana, *Arithmetical applications of an identity for the Vandermonde determinant*, ibid. 130 (2007), 351–359.

[S] G. Salmon, *Lessons Introductory to the Modern Higher Algebra*, 5th ed., Chelsea, 1885.

D. S. Ramana
Harish-Chandra Research Institute
Jhunsi, Allahabad 211 019, India
E-mail: suri@hri.res.in

Received on 23.1.2008
and in revised form on 29.11.2009 (5622)