A NOTE ON INTEGER SOLUTIONS OF THE DIOPHANTINE EQUATION $x^2 - dy^2 = 1$

by JOHN HUNTER

(Received 1st June, 1956)

In the equation

$$x^2 - dy^2 = 1, \quad \ldots\ldots(1)$$

d is any positive integer which is not a perfect square. For convenience we shall consider only those solutions of (1) for which x and y are both positive. All the others can be obtained from these. In fact, it is well known that if (x_0, y_0) is the minimum positive integer solution of (1), then all integer solutions (x, y) are given by

$$x + y\sqrt{d} = \pm (x_0 + y_0\sqrt{d})^n \qquad (n = 0, \pm 1, \pm 2, \ldots),$$

and, in particular, all positive integer solutions are given by

$$x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n \qquad (n = 1, 2, 3, \ldots).$$

The purpose of this note is to establish a procedure for obtaining solutions of (1) by Newton's method of approximating to the root $\sqrt{d}$ of the equation $f(x) \equiv x^2 - d = 0$.

If x_1 is any positive (for convenience) rational number, then Newton's method gives a sequence (x_n) of rational numbers which is defined by the relation

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{x_n^2 - d}{2x_n} = \frac{x_n^2 + d}{2x_n} \qquad (n \geqslant 1), \quad \ldots\ldots(2)$$

and which converges to $\sqrt{d}$. We first note that if (2) is written in the form $x_{n+1} = p_{n+1}/q_{n+1}$, where p_{n+1} and q_{n+1} are the positive rational numbers defined by

$$p_{n+1} = \frac{x_n^2 + d}{|\, x_n^2 - d \,|}, \quad q_{n+1} = \frac{2x_n}{|\, x_n^2 - d \,|}, \quad \ldots\ldots(3)$$

then it is easily verified that (p_{n+1}, q_{n+1}) is a rational solution of (1) for $n = 1, 2, 3, \ldots$. For $n \geqslant 2$, since $x_n = p_n/q_n$ and $p_n^2 - dq_n^2 = 1$, (3) can be simplified to

$$p_{n+1} = p_n^2 + dq_n^2, \qquad q_{n+1} = 2p_n q_n. \quad \ldots\ldots(4)$$

Thus, corresponding to each positive rational number x_1, (2) provides a sequence of positive rational solutions (p_n, q_n) $(n = 2, 3, 4, \ldots)$ of (1) which, by (4), are such that

$$p_{n+1} + q_{n+1}\sqrt{d} = (p_n + q_n\sqrt{d})^2,$$

and hence, by induction, such that

$$p_{n+1} + q_{n+1}\sqrt{d} = (p_2 + q_2\sqrt{d})^{2^{n-1}}, \quad \ldots\ldots(5)$$

where

$$p_2 = \frac{x_1^2 + d}{|\, x_1^2 - d \,|}, \quad q_2 = \frac{2x_1}{|\, x_1^2 - d \,|}. \quad \ldots\ldots(6)$$

Also, if p_2 and q_2 are integers, then (5) gives a sequence of positive integer solutions of (1).

We now establish some properties of the method in the following lemma.

LEMMA. (i) *p_2 and q_2 are integers if and only if $x_1^2 - d$ divides $2x_1$.*

(ii) *If (p, q) is a given positive rational solution of* (1), *then there are two values of x_1, y_1 and y_1^* say, which give rise, by* (6), *to the solution (p, q), and these have the properties*

$$y_1 > \sqrt{d}. \quad y_1^* < \sqrt{d}, \quad y_1 y_1^* = d, \quad y_1 - y_1^* = 2/q.$$

Proof. (i) If p_2 and q_2 are integers, then x_1^2-d divides $2x_1$. Conversely, if x_1^2-d divides $2x_1$, then q_2 is an integer and, since $\frac{x_1^2+d}{x_1^2-d}=1+\frac{2d}{x_1^2-d}$ and $(x_1^2-d,\ x_1)$ divides d, it follows that p_2 is also an integer.

(ii) We have to determine the values of x_1 for which $p=\frac{x_1^2+d}{|x_1^2-d|}$ and $q=\frac{2x_1}{|x_1^2-d|}$. Suppose first that $x_1^2>d$; then $p=\frac{x_1^2+d}{x_1^2-d}$, $q=\frac{2x_1}{x_1^2-d}$ and hence $x_1^2=\frac{p+1}{p-1}d=\frac{2x_1+qd}{q}$, so that $x_1=\frac{qd}{p-1}$. Similarly, if $x_1^2<d$, then $p=\frac{x_1^2+d}{d-x_1^2}$, $q=\frac{2x_1}{d-x_1^2}$ and $x_1=\frac{qd}{p+1}$. If these values of x_1 are denoted by y_1 and y_1^*, respectively, then $y_1>\sqrt{d}$, $y_1^*<\sqrt{d}$, $y_1y_1^*=\frac{q^2d^2}{p^2-1}=d$, since $p^2-dq^2=1$, and $y_1-y_1^*=\frac{2qd}{p^2-1}=\frac{2}{q}$.

From this last equation it follows that if y_1 and y_1^* are integers, then $q=1$ or 2, and that if $q\geqslant 3$, then y_1 and y_1^* are not both integers.

We now show that for certain values of d a corresponding easily-determined value of x_1 gives rise, by (6), to the minimum positive integer solution of (1). Since d is a positive integer which is not a perfect square, it can be expressed uniquely in the form $d=m^2+r$ where $r\neq 0$, $-m+1\leqslant r\leqslant m$, for some positive integer m.

THEOREM. (i) *If* $r=-1$, *then* $x_1=m-1$ *gives the minimum positive integer solution of* (1), *and this is* $(m,\ 1)$.

(ii) *If* r *divides* $2m$, $r\neq -1$, *then* $x_1=m$ *gives the minimum positive integer solution of* (1), *and this is* $\left(\frac{2m^2+r}{|r|},\ \frac{2m}{|r|}\right)$.

Proof. (i) In this case, $d-x_1^2=2(m-1)$, $d+x_1^2=2m(m-1)$ and, by (6), $p_2=m$, $q_2=1$, and this is clearly the minimum positive integer solution.

(ii) Here $|x_1^2-d|=|r|$, so that x_1^2-d divides $2x_1$ and thus, by part (i) of the above lemma, p_2 and q_2 are integers. From (6), $p_2=\frac{2m^2+r}{|r|}$ and $q_2=\frac{2m}{|r|}$. Suppose now that $(x_0,\ y_0)$ is the minimum positive integer solution of (1). Then the second minimum positive integer solution is $(x_0^2+dy_0^2,\ 2x_0y_0)$, that is $(1+2dy_0^2,\ 2x_0y_0)$. Now $1+2dy_0^2\geqslant 1+2d$; but

$$\frac{2m^2+r}{|r|}=\frac{2d-r}{|r|}\leqslant\frac{2}{|r|}d+1<2d+1 \quad \text{if } |r|>1,$$

and also

$$\frac{2m^2+r}{|r|}=2d-1<2d+1 \quad \text{if } r=1.$$

Hence the positive integer solution $(p_2,\ q_2)$ is the minimum positive integer solution.

It is of interest to note that the results of this theorem give the minimum positive integer solutions of (1) for all values of d in the range $2\leqslant d\leqslant 40$ except for $d=13,\ 19,\ 21,\ 22,\ 28,\ 29$ and 31.

We note finally that the results in the theorem are not new (see, for example, L. E. Dickson's *History of the theory of numbers*, II, p. 378). It is surprising that no account of the relation of Newton's method to the equation $x^2-dy^2=1$ appears to exist in the literature.

THE UNIVERSITY
GLASGOW