A METHOD FOR SOLVING CERTAIN DIOPHANTINE EQUATIONS

W. H. MILLS

In this paper a simple method is presented for solving completely the Diophantine equation

$$x^2 + xyz + \epsilon y^2 + ax + by + c = 0, \tag{1}$$

where $\epsilon = \pm 1$ and a, b, c are integers. The special case $x^2+xyz+y^2+c = 0$ has recently been treated by Barnes [1], using methods developed by Mordell [3]. The case $\epsilon=c=1$, $a=b$ has been treated independently but by the same method [2]. In this paper we use a modification of the methods of [1] and [2] that enables us to treat the more general equation (1).

1. Let $x=x_1$, $y=y_1$, $z=\alpha$ be an integral solution of (1). If we put $y=y_1$, $z=\alpha$ in (1) and solve for x, we obtain the two roots x_1 and $x_2 = -\alpha y_1-a-x_1$. Clearly $x=x_2$, $y=y_1$, $z=\alpha$ is another solution of (1). In the same manner $x=x_2$, $y=y_2$, $z=\alpha$ is a third integral solution, where

$$y_2 = (-\alpha x_2 - b)/\epsilon - y_1 = -\epsilon(\alpha x_2 + b) - y_1.$$

Continuing in this way we obtain a sequence S, $\cdots$, x_1, y_1, x_2, y_2, $\cdots$, such that

$$x_n + x_{n+1} = -\alpha y_n - a \tag{2}$$

and

$$y_n + y_{n+1} = -\epsilon(\alpha x_{n+1} + b). \tag{3}$$

It is clear that S can be extended arbitrarily far in either direction, and that for any n,

$$x = x_n, \qquad y = y_n, \qquad z = \alpha \tag{4}$$

and

$$x = x_{n+1}, \qquad y = y_n, \qquad z = \alpha \tag{5}$$

are integral solutions of (1). We shall call such a sequence a solution sequence of (1) corresponding to α. We shall say that the solutions (4) and (5) are the solutions belonging to S. We consider two solution sequences S and S' identical if and only if every solution belong-

Received by the editors October 1, 1953.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

ing to S also belongs to S' and conversely. This is clearly the case when there is a single solution belonging to both of them.

There need not be an infinite number of solutions belonging to a given solution sequence S since S may be cyclic. In fact there may be only one solution belonging to a given solution sequence [2, p. 217].

We note that once a pair of consecutive elements of a solution sequence corresponding to a given value of α is known, it is a simple matter to obtain an expression for the general term. From (2) and (3) we obtain easily

$$x_{n-1} + (2 - \alpha^2\epsilon)x_n + x_{n+1} - b\alpha\epsilon + 2a = 0,$$

and this can be solved by difference equation methods.

2. Suppose now that $x^2+ax+c=0$ has a rational root β. Then $x=\beta$, $y=0$, $z=\alpha$ is an integral solution of (1) for every integer α. A similar result holds if $\epsilon y^2+by+c=0$ has a rational root. Thus we see that if either $x^2+ax+c=0$ or $\epsilon y^2+by+c=0$ has a rational root, then there exists at least one solution sequence corresponding to any integral value of z. On the other hand we can prove the following result:

FINITENESS THEOREM. *If x^2+ax+c and ϵy^2+by+c are both irreducible over the field of rational numbers, then there are only a finite number of solution sequences of* (1).

PROOF. Let S be any solution sequence of (1). Without loss of generality we can suppose that either x_1 or y_1 is an element of S of minimum absolute value. Suppose first that y_1 is such an element. Since x^2+ax+c is irreducible it follows that $y_1 \neq 0$. Now

$$x_1x_2 = \epsilon y_1^2 + by_1 + c \tag{6}$$

and $|x_2| \geqq |y_1|$. Hence $|x_1| \leqq |y_1| + |b| + |c|$. Therefore we can write $x_1=\epsilon_1y_1+\delta_1$ where $\epsilon_1 = \pm 1$ and $|\delta_1| \leqq |b| + |c|$. Similarly $x_2=\epsilon_2y_1+\delta_2$ where $\epsilon_2 = \pm 1$ and $|\delta_2| \leqq |b| + |c|$. Substituting in (6) we obtain

$$\epsilon y_1^2 + by_1 + c = (\epsilon_1y_1 + \delta_1)(\epsilon_2y_1 + \delta_2).$$

Since ϵy^2+by+c is irreducible there are at most two possibilities for y_1 for each possible combination of ϵ_1, ϵ_2, δ_1, δ_2. Since there are at most $4(2|b|+2|c|+1)^2$ such combinations we see that there are at most $8(2|b|+2|c|+1)^2$ solution sequences such that y_1 is an element of minimal absolute value. Similarly there are at most $8(2|a|+2|c|+1)^2$ solution sequences such that x_1 is an element of minimal abso-

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

lute value. Therefore there are at most $8(2|b|+2|c|+1)^2+8(2|a|+2|c|+1)^2$ solution sequences. Thus the theorem is established.

The argument used in the proof of the finiteness theorem can be used to determine all solution sequences of (1) regardless of the reducibility of x^2+ax+c and ϵy^2+by+c. Thus (1) can be completely solved by this method for any particular values of a, b, c, and ϵ.

These methods shed some additional light on quadratic Diophantine equations. For example we note the following immediate consequence of the finiteness theorem.

COROLLARY. *If a, b, and c are fixed rational integers, $\epsilon=\pm 1$, and if x^2+ax+c and ϵy^2+by+c are both irreducible over the field of rational numbers, then*

$$x^2 + \alpha xy + \epsilon y^2 + ax + by + c = 0$$

has integral solutions for at most a finite number of values of α.

REFERENCES

1. E. S. Barnes, *On the Diophantine equation $x^2+y^2+c=xyz$*, J. London Math. Soc. vol. 28 (1953) pp. 242–244.

2. W. H. Mills, *A system of quadratic Diophantine equations*, Pacific Journal of Mathematics vol. 3 (1953) pp. 209–220.

3. L. J. Mordell, *The congruence $ax^3+by^3+c\equiv 0 \pmod{xy}$, and integer solutions of cubic equations in three variables*, Acta Math. vol. 88 (1952) pp. 77–83.

YALE UNIVERSITY

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use