A METHOD FOR SOLVING CERTAIN DIOPHANTINE EQUATIONS

W. H. MILLS

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

\[
x^2 + xyz + \epsilon y^2 + ax + by + c = 0,
\]

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

\[
y_2 = (-\alpha x_2 - b)/\epsilon - y_1 = -\epsilon(ax_2 + b) - y_1.
\]

Continuing in this way we obtain a sequence \(S, \ldots, x_1, \ y_1, \ x_2, \ y_2, \ldots\), such that

\[
(2) \quad x_n + x_{n+1} = -\alpha y_n - a
\]

and

\[
(3) \quad y_n + y_{n+1} = -\epsilon(ax_{n+1} + b).
\]

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

\[
(4) \quad x = x_n, \quad y = y_n, \quad z = \alpha
\]

and

\[
(5) \quad x = x_{n+1}, \quad y = y_n, \quad z = \alpha
\]

are integral solutions of (1). We shall call such a sequence a solution sequence of (1) corresponding to \(\alpha\). 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.
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 \( \alpha \) 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 \( \beta \). Then \( x = \beta, y = 0, z = \alpha \) is an integral solution of (1) for every integer \( \alpha \). A similar result holds if \( \epsilon y^2 + \beta y + c = 0 \) has a rational root. Thus we see that if either \( x^2 + ax + c = 0 \) or \( \epsilon y^2 + \beta y + c = 0 \) 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 \( \epsilon y^2 + \beta y + c \) 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

\[
x_1 x_2 = \epsilon y_1 + b y_1 + c
\]

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

\[
\epsilon y_1 + b y_1 + c = (\epsilon_1 y_1 + \delta_1)(\epsilon_2 y_1 + \delta_2).
\]

Since \( \epsilon y^2 + \beta y + c \) is irreducible there are at most two possibilities for \( y_1 \) for each possible combination of \( \epsilon_1, \epsilon_2, \delta_1, \delta_2 \). 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-
olute 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 $ey^2+by+c$. Thus (1) can be completely solved by this method for any particular values of $a$, $b$, $c$, and $e$.

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, $e = \pm 1$, and if $x^2+ax+c$ and $ey^2+by+c$ are both irreducible over the field of rational numbers, then

$$x^2 + axy + ey^2 + ax + by + c = 0$$

has integral solutions for at most a finite number of values of $\alpha$.

**References**


**Yale University**