# CERTAIN DIOPHANTINE EQUATIONS LINEAR IN ONE UNKNOWN

W. H. MILLS

**1. Introduction.** A. Brauer and R. Brauer **(2)** and Barnes **(1)** (following a method of Mordell **(6)**) have solved the Diophantine equation $x^2+y^2+c = xyz$ subject to the condition $(x, y) = 1$. Independently, but using the same methods, I treated **(4)** the equation

$$x^2+y^2+ax+ay+1 = xyz,$$

and subsequently **(5)** gave a method of obtaining all integral solutions of

$$x^2 \pm y^2+ax+by+c = xyz,$$

thereby generalizing **(2)**, **(1)**, and **(4)**. Recently Goldberg, Newman, Straus, and Swift **(3)** have treated the equation

$$ax^2+bxy+cy^2 = (p+qxy)z,$$

where $a$, $b$, $c$, $p$, and $q$ are integers satisfying the divisibility conditions $a|(b, q)$ and $c|(b, q)$. In the present paper we combine the methods of **(3)** and **(5)**. This enables us to obtain the complete solution of the Diophantine equation

$$ax^2+bxy+cy^2+dx+ey+f = z(pxy+qx+ry+s), \tag{1}$$

where $a$, $b$, $c$, $d$, $e$, $f$, $p$, $q$, $r$, and $s$ are integers satisfying the divisibility conditions $a|(b, d, p, q)$ and $c|(b, e, p, r)$, and $p \neq 0$. This generalizes all the previous results.

The solutions of (1) can be divided into classes, such that once one solution belonging to a given class is known the others can be determined recursively. In fact, after one solution is known, the others belonging to the same class can be determined explicitly by solving a pair of linear difference equations. Thus the problem is reduced to finding one solution in each class. All solutions in the same class have the same value of $z$. For sufficiently large numerical values of $z$ there is a solution in each class for which either $x = -r/p$ or $y = -q/p$, or for which both sides of (1) vanish. This makes it easy to give necessary and sufficient conditions for (1) to have solutions for an infinite number of different values of $z$, and means that for large numerical values of $z$ the solutions of (1) can be readily obtained. Since for particular values of $z$ the equation (1) is a quadratic Diophantine equation in two variables, which can be solved in integers by classical methods, we see that the complete solution of (1) can always be obtained in a finite number of steps. It is not necessary to use classical quadratic equation methods to solve (1) for particular values of

Received March 5, 1955.

$z$. A method more in line with the spirit of this paper is developed in §4. For a fixed value of $z$ there can be only a finite number of solution classes except in two simple special cases.

Goldberg, Newman, Straus, and Swift have pointed out **(3)** that if the divisibility conditions are not satisfied the solution has an entirely different character. The present methods give only an incomplete solution in this case.

**2. Construction of $\alpha$-sequences.** Let us put

$$N(x, y) = ax^2+bxy+cy^2+dx+ey+f, \qquad D(x, y) = pxy+qx+ry+s,$$

where all the coefficients are rational integers, $p \neq 0$, and

$$a|(b, d, p, q), \qquad c|(b, e, p, r). \tag{2}$$

These conditions imply that $a \neq 0$ and $c \neq 0$. We consider the Diophantine equation

$$N(x, y) = zD(x, y). \tag{3}$$

Let $x = u_0$, $y = u_1$, $z = \alpha$ be an integral solution of (3). Then

$$N(x, u_1) = \alpha D(x, u_1) \tag{4}$$

is a quadratic equation in $x$ with roots $x = u_0$ and $x = u_2$, where $u_2$ satisfies

$$a(u_0+u_2) = pu_1\alpha+q\alpha-bu_1-d. \tag{5}$$

It follows from (2) that $u_0+u_2$ is an integer. Therefore $x = u_2$, $y = u_1$, $z = \alpha$ is also an integral solution of (3). Continuing in this manner we obtain a sequence

$$\ldots, u_0, u_1, u_2, u_3, \ldots \tag{6}$$

where

$$a(u_{2n}+u_{2n+2}) = pu_{2n+1}\alpha+q\alpha-bu_{2n+1}-d, \tag{7}$$

and

$$c(u_{2n-1}+u_{2n+1}) = pu_{2n}\alpha+r\alpha-bu_{2n}-e. \tag{8}$$

It is clear that (6) can be extended infinitely far in either direction and that $x = u_{2n}$, $y = u_{2n\pm1}$, $z = \alpha$ are integral solutions of (3) for every integer $n$. We will call such a sequence an *$\alpha$-sequence* of (3). We consider two $\alpha$-sequences identical if they lead to the same solutions of (3).

We need the following result:

LEMMA. *If $|u_2| \geqslant |u_0|$, then either $pu_1+q = 0$ or*

$$|u_0| \leqslant |c/a|^{\frac{1}{2}}|u_1|+C,$$

*where $C$ is a constant depending only on the coefficients of $N(x, y)$ and $D(x, y)$.*

*Proof.* Since $u_0$ and $u_2$ are the roots of (4), we have (5) and

$$au_0\,u_2 = cu_1^2+eu_1+f-\alpha(ru_1+s). \tag{9}$$

https://doi.org/10.4153/CJM-1956-003-2 Published online by Cambridge University Press

Eliminating $\alpha$ from (5) and (9) we obtain

$$au_2D(u_0, u_1)+au_0(ru_1+s) = cpu_1^3+Q(u_1),$$

where $Q(u_1)$ is a quadratic polynomial in $u_1$ with constant coefficients, i.e., coefficients that depend only on $a, b, c, d, e, f, p, q, r$, and $s$. Since $|u_2| \geqslant |u_0|$, we have

$$\begin{aligned}|cpu_1^3 + Q(u_1)| &\geqslant |au_0D(u_0, u_1)| - |au_0(ru_1 + s)| \\ &\geqslant |a(pu_1 + q)\, u_0^2| - 2|a(ru_1 + s)\, u_0|.\end{aligned}$$

Therefore, if $pu_1+q \neq 0$, the quadratic formula yields

$$\begin{aligned}|u_0| &\leqslant |pu_1+q|^{-1}\{|(ru_1+s)| + (|(ru_1+s)|^2 + |a^{-1}(pu_1 + q)(cpu_1^3 + Q(u_1)|)^{\frac{1}{2}}\} \\ &\leqslant |c/a|^{\frac{1}{2}}|u_1| + C,\end{aligned}$$

where $C$ is a positive constant depending only on the coefficients of $N(x, y)$ and $D(x, y)$. This proves the Lemma.

**3. Classification of $\alpha$-sequences.** We will distinguish four types of $\alpha$-sequences.

*Type* I. We will say that an $\alpha$-sequence is a *type* I *sequence* if $D(u_{2k}, u_{2k+1}) = 0$ or $D(u_{2k}, u_{2k-1}) = 0$ for some integer $k$. It is clear that there exist type I sequences of (3) if and only if the system

$$D(x, y) = N(x, y) = 0 \tag{10}$$

has an integral solution. Each integral solution of (10) leads to an $\alpha$-sequence of (3) for every integer $\alpha$. Since $pac \neq 0$, (10) has at most four solutions, and so there are at most four type I $\alpha$-sequences for any particular value of $\alpha$.

*Type* II. We will say that an $\alpha$-sequence is a *type* II *sequence* if

$$pu_{2k+1}+q = 0, \qquad ru_{2k+1}+s \neq 0 \tag{11}$$

for some integer $k$. We see that (11) implies $p|q$, $ps \neq qr$, and $N(u_{2k}, -q/p) = \alpha(ps - qr)/p$. Thus there exist type II sequences of (3) if and only if $p|q$, $ps \neq qr$, and the congruence

$$pN(x, -q/p) \equiv 0 \pmod{ps - qr}$$

has integral solutions. If type II sequences exist, then there exist $\alpha$-sequences of type II for an infinite number of different values of $\alpha$, namely for every integer $\alpha$ that can be represented in the form $pN(x, -q/p)/(ps - qr)$ with integral $x$.

*Type* IIA. We will say that an $\alpha$-sequence is of *type* IIA if $pu_{2k} + r = 0$ and $qu_{2k} + s \neq 0$ for some integer $k$. Interchanging the roles of $x$ and $y$ interchanges the type II and the type IIA sequences. Therefore the discussion of type II sequences can be applied directly to the type IIA sequences.

It is clearly a straightforward matter to determine all type I, II, and IIA sequences for any given numerical values of the parameters $a$, $b$, $c$, $d$, $e$, $f$, $p$, $q$, $r$, and $s$.

*Type* III. If an $\alpha$-sequence is not of type I, II, or IIA, we say that it is a *type* III *sequence.*

THEOREM 1. *There are $\alpha$-sequences of type* III *for only a finite number of different values of $\alpha$.*

*Proof.* Let $\{u_m\}$ be a type III sequence. Without loss of generality we suppose that $u_1$ is an element of $\{u_m\}$ of least absolute value. (This may involve interchanging the roles of $x$ and $y$.) Furthermore we may suppose that $|u_2| \geqslant |u_0|$.

If $pu_1 + q = 0$ and $ru_1 + s = 0$, then $D(u_0, u_1) = 0$. Hence, since $\{u_m\}$ is neither of type I nor of type II, we have $pu_1 + q \neq 0$. Therefore $|u_0| \leqslant |c/a|^{\frac{1}{2}} |u_1| + C$ by the Lemma of §2. Also, since $|u_1|$ is minimal, we have $|u_1| \leqslant |u_0|$. We now distinguish two cases:

*Case* 1. $|pu_0 u_1| \leqslant 2|qu_0 + ru_1 + s|$. Here

$$|pu_0 u_1| \leqslant 2(|q|\,|c/a|^{\frac{1}{2}} + |r|)|u_1| + 2|q|C + 2|s|.$$

Hence if $u_1 \neq 0$ we have $|u_1| \leqslant |u_0| \leqslant D$ for some constant $D$, while if $u_1 = 0$ we have $|u_0| \leqslant C$. Thus both $|u_0|$ and $|u_1|$ are bounded, and hence there are only a finite number of possible values for $\alpha = N(u_0, u_1)/D(u_0, u_1)$.

*Case* 2. $|pu_0 u_1| > 2|qu_0 + ru_1 + s|$. Here $|D(u_0, u_1)| > \frac{1}{2}|pu_0 u_1|$, $u_0 \neq 0$, $u_1 \neq 0$, and so

$$|p\alpha| = \frac{|pN(u_0, u_1)|}{|D(u_0, u_1)|} < 2\frac{|au_0|}{|u_1|} + 2|b| + 2|c| + 2|d| + 2|e| + 2|f|,$$

which is bounded since $|u_0/u_1| \leqslant |c/a|^{\frac{1}{2}} + C$. This completes the proof of Theorem 1.

As a direct result of Theorem 1 and the elementary properties of type I, II, and IIA sequences we obtain:

THEOREM 2. *A necessary and sufficient condition for* (3) *to have integral solutions for an infinite number of different values of $z$ is that either*

(i) *the system $N(x, y) = D(x, y) = 0$ has at least one integral solution, or*

(ii) *$p|q$, $ps \neq qr$, and the congruence $pN(x, -q/p) \equiv 0 \pmod{ps - qr}$ has at least one integral solution, or*

(iii) *$p|r$, $ps \neq qr$, and the congruence $pN(-r/p, y) \equiv 0 \pmod{ps - qr}$ has at least one integral solution.*

Special cases of Theorem 2 can be found in **(3)**, **(4)**, and **(5)**.

**4. The $\alpha$-sequences for a fixed value of $\alpha$.** We proved in the last section that, for any fixed values of the coefficients of $N(x, y)$ and $D(x, y)$, the possible

https://doi.org/10.4153/CJM-1956-003-2 Published online by Cambridge University Press

values of $z$ are bounded except for a limited number of infinite classes of sequences, which can be readily determined. To obtain the complete solution of (3) we need an effective method of determining all $\alpha$-sequences for a fixed value of $\alpha$. In this section we will discuss such a method.

Let $\{u_m\}$ be an $\alpha$-sequence of (3). Put $b' = b - p\alpha$, $d' = d - q\alpha$, $e' = e - r\alpha$, and $f' = f - s\alpha$. Then (3) becomes

$$ax^2 + b'xy + cy^2 + d'x + e'y + f' = 0,$$

and the divisibility conditions (2) yield

$$a|(b', d') \qquad c|(b', e'). \tag{12}$$

Furthermore (7) and (8) become

$$a(u_{2n} + u_{2n+2}) = -b'u_{2n+1} - d', \tag{13}$$

and

$$c(u_{2n-1} + u_{2n+1}) = -b'u_{2n} - e'. \tag{14}$$

If we eliminate $u_1$ from $a(u_0 + u_2) = -b'u_1 - d'$ and

$$au_0u_2 = cu_1^2 + e'u_1 + f',$$

which is obtained from (9), then we get $G(u_0, u_2) = 0$, where

$$G(u, v) = u^2 + Buv + v^2 + Du + Dv + F,$$

$B = 2 - b'^2/ac$, $D = (2cd' - b'e')/ac$, and

$$F = (cd'^2 + b'^2f' - b'd'e')/a^2c.$$

It follows from (12) that $B$ and $D$ are integers. Hence $F$ must be an integer. From (13) and (14) we obtain

$$\begin{aligned} ac(u_{2n} + 2u_{2n+2} + u_{2n+4}) &= -b'c(u_{2n+1} + u_{2n+3}) - 2cd' \\ &= b'^2u_{2n+2} + b'e' - 2cd'. \end{aligned}$$

Therefore

$$u_{2n} + u_{2n+4} = -Bu_{2n+2} - D. \tag{15}$$

It follows that $x = u_0$ and $x = u_4$ are the roots of $G(x, u_2) = 0$, and hence

$$u_0u_4 = u_2^2 + Du_2 + F. \tag{16}$$

Now we may suppose, without loss of generality, that $|u_2| \leqslant |u_{2n}|$ for all $n$. In particular $|u_0| \geqslant |u_2|$ and $|u_4| \geqslant |u_2|$, and so we may write

$$u_0 = \epsilon u_2 + \delta, \qquad u_4 = \epsilon' u_2 + \delta',$$

where

$$\epsilon = \pm 1, \qquad \epsilon' = \pm 1, \qquad \epsilon u_2\,\delta \geqslant 0, \qquad \epsilon' u_2\,\delta' \geqslant 0. \tag{17}$$

Substituting in (15) and (16) we obtain

$$-Bu_2 - D = (\epsilon + \epsilon')u_2 + \delta + \delta', \tag{18}$$

https://doi.org/10.4153/CJM-1956-003-2 Published online by Cambridge University Press

and

$$u_2^2 + Du_2 + F = \epsilon\epsilon' u_2^2 + \epsilon\delta' u_2 + \epsilon'\delta u_2 + \delta\delta'. \tag{19}$$

Every non-zero term on the right hand side of (19) has the same sign by (17). Therefore

$$|Du_2 + F| \geqslant |\delta' u_2| + |\delta u_2|. \tag{20}$$

If $u_2 \neq 0$, then (20) yields $|\delta| + |\delta'| \leqslant |D| + |F|$, and there are only a finite number of possibilities for $\epsilon$, $\epsilon'$, $\delta$, and $\delta'$. From (18) and (19) we see that for any fixed values of $\epsilon$, $\epsilon'$, $\delta$, and $\delta'$ there are at most two values of $u_2$ unless

$$\begin{aligned} &\epsilon + \epsilon' = -B, \quad \delta + \delta' = -D, \\ &\epsilon\epsilon' = 1, \quad \epsilon\delta' + \epsilon'\delta = D, \quad \delta\delta' = F. \end{aligned} \tag{21}$$

Thus, unless (21) has an integral solution, there are only a finite number of possible values for $u_2$. Each value of $u_2$ leads to at most one $\alpha$-sequence. Hence if (21) has no integral solution, then there are at most a finite number of $\alpha$-sequences, and they can all be found in a finite number of steps.

Suppose that (21) holds. Then $\epsilon = \epsilon' = \pm 1$.

(i) $\epsilon = \epsilon' = 1$. Here we have $B = -2$, $-D = \delta + \delta' = D$, and $\delta\delta' = F$. Hence $D = 0$. Ignoring the possibility $u_2 = 0$, which leads to at most one $\alpha$-sequence, we obtain $\delta = \delta' = 0$ from $\delta + \delta' = 0$ and (17). Therefore

$$B = -2, \quad D = F = 0. \tag{22}$$

It is easily seen that (22) is equivalent to

$$4a(ax^2 + b'xy + cy^2 + d'x + e'y + f') = (2ax + b'y + d')^2. \tag{23}$$

Conversely suppose (23) holds. Then, since $u_{2n}$ and $u_{2n+2}$ are the roots of $(2ax + b'u_{2n+1} + d')^2 = 0$, we see that $u_{2n} = u_{2n+2}$. Similarly $u_{2n-1} = u_{2n+1}$. Therefore $u_m = u_{m+2}$ for all $m$, and so in this case every $\alpha$-sequence is cyclic of period 1 or 2. Furthermore, since $B = -2$, we have $(b - p\alpha)^2 = 4ac$, and thus this type of behavior can occur for at most two values of $\alpha$, namely $\alpha = (b \pm 2\sqrt{ac})/p$.

(ii) $\epsilon = \epsilon' = -1$. Here (21) yields $B = 2$, and so $b' = 0$. Conversely suppose $b' = 0$. Then $\alpha = b/p$. Here (13) gives us

$$u_{2n} + u_{2n+2} = -d'/a$$

for all $n$. Hence $u_{2n} = u_{2n+4}$. Similarly from (14) we obtain $u_{2n-1} = u_{2n+3}$. Therefore $u_m = u_{m+4}$ for all $m$. If $u_m = u_{m+2}$ for all $m$, then $u_0 = -d'/2a$, $u_1 = -e'/2c$, and so the conic

$$ax^2 + cy^2 + d'x + e'y + f' = 0$$

degenerates either to a single point or to a pair of intersecting straight lines. Therefore if $b' = 0$ every $\alpha$-sequence is cyclic, and with at most one exception every $\alpha$-sequence has period exactly 4. We have proved:

THEOREM 3. *If* (3) *has an infinite number of* $\alpha$*-sequences for a fixed value of* $\alpha$, *then either*

(i) $\alpha = (b \pm 2\sqrt{ac})/p$, $N(x, y) - \alpha D(x, y)$ *is a constant times a perfect square, and every* $\alpha$*-sequence is of period* 1 *or* 2, *or*

(ii) $\alpha = b/p$, $N(x, y) - \alpha D(x, y)$ *has no* $xy$ *term, and with at most one exception every* $\alpha$*-sequence has period exactly* 4.

Using the methods of §3 and §4 all $\alpha$-sequences of (3) can be found in a finite number of steps. In particular cases short cuts are frequently available, and sometimes it is but the work of a few lines to determine all $\alpha$-sequences **(3; 4)**.

**5. Cyclic $\alpha$-sequences.** We observed in the last section that

$$u_{2n} + Bu_{2n+2} + u_{2n+4} + D = 0. \tag{24}$$

Hence if $B = -2$, then $u_{2n}$ is a quadratic function of $n$. If $B = 2$, then $b' = 0$, and we know that in this case $\{u_m\}$ is cyclic of period 1, 2, or 4. Now if $B \neq \pm 2$, then the general solution of the difference equation (24) is

$$u_{2n} = C_1\epsilon_1^n + C_2\epsilon_2^n - D/(B + 2),$$

where $\epsilon_1$ and $\epsilon_2$ are the roots of $x^2 + Bx + 1 = 0$, and $C_1$ and $C_2$ are arbitrary. Hence if $|B| > 2$, the sequence $\{u_{2n}\}$ is non-cyclic unless $C_1 = C_2 = 0$, in which case $u_{2n+2} = u_{2n}$. For $B = 1, 0$, and $-1$, $\epsilon_1$ and $\epsilon_2$ are the primitive 3rd, 4th, and 6th roots of unity respectively. Thus if $B = 1$, then $u_{2n+6} = u_{2n}$; if $B = 0$, then $u_{2n+8} = u_{2n}$; and if $B = -1$, then $u_{2n+12} = u_{2n}$. Since the identical statements hold for elements of the form $u_{2n+1}$, with $D$ replaced by $(2ce' - b'd')/ac$ but with the same value of $B$, we have the following result:

THEOREM 4. *If an* $\alpha$*-sequence is cyclic it has period* 1, 2, 3, 4, 6, 8, *or* 12.

All $\alpha$-sequences have been determined in **(4)** for

$$x^2 + y^2 + dx + dy + 1 = xyz, \qquad 0 \leqslant d \leqslant 10.$$

They include cyclic sequences of periods 1, 2, 3, 4, and 6, as well as many non-cyclic sequences.

If $a = 1$, $b' = c = 2$, $d' = e' = 0$, $f = -10$, there is a cyclic sequence of period 8 with $u_0 = 2$, $u_1 = 1$:

$$\ldots, 2, 1, -4, 3, -2, -1, 4, -3, 2, 1, \ldots.$$

If $a = 1$, $b' = c = 3$, $d' = e' = 0$, $f = -13$, there is a cyclic sequence of period 12 with $u_0 = 2$, $u_1 = 1$:

$$\ldots, 2, 1, -5, 4, -7, 3, -2, -1, 5, -4, 7, -3, 2, 1, \ldots.$$

Thus we see that all the possible periods listed in Theorem 4 actually occur.

Additional examples and special cases of the results of this paper can be found in **(1; 2; 3; 4;** and **5)**.

https://doi.org/10.4153/CJM-1956-003-2 Published online by Cambridge University Press

## References


1. E. S. Barnes, *On the Diophantine equation* $x^2 + y^2 + c = xyz$, J. London Math. Soc., *28* (1953), 242–244.
2. A. Brauer and R. Brauer, *Lösung der Aufgabe* 46, Angelegenheiten d. Deutschen Mathem.-Vereinigung, (1927), 90–92 (Jahresbericht d. Deutschen Mathem.-Vereinigung, *36*).
3. Karl Goldberg, Morris Newman, E. G. Straus, and J. D. Swift, *The representation of integers by binary quadratic rational forms*, Archiv der Mathematik, *5* (1954), 12–18.
4. W. H. Mills, *A system of quadratic Diophantine equations*, Pacific J. Math., *3* (1953), 209–220.
5. ———, *A method for solving certain Diophantine equations*, Proc. Amer. Math. Soc., *5* (1954), 473–475.
6. 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., *88* (1952), 77–83.


*Yale University*