Pacific Journal of Mathematics

A SYSTEM OF QUADRATIC DIOPHANTINE EQUATIONS

WILLIAM H. MILLS

Vol. 3, No. 1 March 1953

A SYSTEM OF QUADRATIC DIOPHANTINE EQUATIONS

W. H. MILLS

1. Introduction. In spite of the efforts of many mathematicians of the last 300 years, comparatively few general methods of solving nonlinear Diophantine equations are available, and much of the literature on the subject consists of isolated results. When it comes to systems of simultaneous nonlinear Diophantine equations, the results become even more fragmentary, and a complete solution of such a system is a rarity. In this paper we study a pair of simultaneous quadratic Diophantine equations that can be solved easily and completely by difference equation methods.

The system in question,

$$x \mid y^2 + ay + 1, \quad y \mid x^2 + ax + 1, \tag{1}$$

where a is a fixed integer, is essentially a pair of simultaneous quadratic equations in four unknowns. This system is equivalent to a nonlinear second order difference equation. Furthermore, every solution of this nonlinear difference equation is also a solution of a linear difference equation with constant coefficients. We can thus obtain the complete solution of (1) in integers. With some additional effort we can obtain all positive integral solutions.

The principal result is that if $a \neq \pm 2$, then there exists a finite number of sequences such that x and y satisfy (1) if and only if they are consecutive terms of one of these sequences. These sequences are similar to the Fibonacci sequence in that there is a linear relation connecting any three consecutive terms. For the special case $a = 0$, we obtain the following result: x and y are positive integers such that

$$x \mid y^2 + 1 \quad \text{and} \quad y \mid x^2 + 1$$

if and only if x and y are consecutive elements of the sequence 1, 1, 2, 5, 13, 34, $\cdots$ obtained from the classical Fibonacci sequence by striking out alternate terms. For $a = \pm 2$, the chief differences are that there is an infinite number of sequences and that 0 can be a term of a sequence.

Received July 10, 1951.
Pacific J. Math. 3 (1953), 209-220

Clearly the system (1) is closely related to the quadratic Diophantine equations of the type

$$x^2 - \alpha xy + y^2 + ax + ay + 1 = 0. \tag{2}$$

An easy consequence of our main results is that for fixed $a \neq \pm 2$, (2) has integral solutions for only a finite number of integral values of α. These values of α can easily be found by the methods of this paper.

It is possible that similar methods can be used to obtain further insight into the general quadratic Diophantine equation in two unknowns. At any rate, there is a large class of such equations that can be completely and easily solved this way, and partial solutions can be obtained to many others.

2. Preliminary discussion. Let a be a fixed rational integer. Let x and y be rational integers satisfying (1). Then there exists an integer z such that

$$xz = y^2 + ay + 1. \tag{3}$$

Now $xz \equiv 1 \pmod{y}$ and hence

$$x^2(z^2 + az + 1) \equiv 1 + ax + x^2 \equiv 0 \pmod{y}.$$

Furthermore, x and y are relatively prime. Thus we have

$$y \mid z^2 + az + 1 \quad \text{and} \quad z \mid y^2 + ay + 1.$$

Continuing in this manner, we obtain a chain $\cdots, x, y, z, \cdots$ such that any two consecutive terms satisfy (1), and any three consecutive terms satisfy (3). We note that x and y determine z uniquely except when $x = 0$.

DEFINITION. A sequence of integers $\{u_i\}$ with at least three terms,

$$\cdots, u_1, u_2, u_3, \cdots,$$

is an *a-chain* if (A) any three consecutive terms satisfy the nonlinear difference equation

$$u_{n+1} u_{n-1} = u_n^2 + au_n + 1, \tag{4}$$

and (B) $u_n = 0$ if and only if u_n is either the first or the last term in the sequence.

We shall consider two a-chains $\{u_i\}$ and $\{v_i\}$ the same, if and only if there exists an h such that either $u_n = v_{h+n}$ for all n or $u_n = v_{h-n}$ for all n.

It is clear that two integers x and y satisfy (1) if and only if they are consecutive integers of an a-chain. Furthermore any two consecutive nonzero terms of an a-chain determine it completely. Thus the solution of (1) is reduced to the problem of determining all a-chains.

3. The finiteness theorem. We shall now establish the following theorem.

THEOREM 1. *If $a \neq \pm 2$ there is only a finite number of a-chains.*

Proof. Let $\{u_i\}$ be an a-chain. Since $a \neq \pm 2$, it follows that $u_n \neq 0$ for all n, and that $\{u_i\}$ has neither a first nor a last element. Without loss of generality we may suppose that

$$|u_n| \geq |u_1| \geq 1$$

for all n. Now

$$|u_1^2| + |au_1| + 1 \geq |u_1^2 + au_1 + 1| = |u_2 u_0| \geq |u_1 u_0|.$$

Hence

$$|u_1| + |a| + 1 \geq |u_0| \geq |u_1|.$$

Therefore we can write

$$u_0 = \epsilon_1 u_1 + b,$$

where $\epsilon_1 = \pm 1$ and $|b| \leq |a| + 1$. Similarly,

$$u_2 = \epsilon_2 u_1 + c,$$

where $\epsilon_2 = \pm 1$ and $|c| \leq |a| + 1$. There are at most $4(2|a| + 3)^2$ ways of choosing ϵ_1, ϵ_2, b, and c. Now

$$u_1^2 + au_1 + 1 = u_0 u_2 = \epsilon_1 \epsilon_2 u_1^2 + (b\epsilon_2 + c\epsilon_1) u_1 + bc.$$

Thus for each choice of ϵ_1, ϵ_2, b, and c there are at most two values of u_1, except when

$$\epsilon_1 \epsilon_2 = 1, \quad b\epsilon_2 + c\epsilon_1 = a, \quad \text{and} \quad bc = 1.$$

In this case we have

$$\epsilon_1 = \epsilon_2 = \pm 1, \quad b = c = \pm 1,$$

and hence $a = \pm 2$. Thus if $a \neq \pm 2$ the number of a-chains is not more than $8(2|a| + 3)^2$, and the theorem is proved.

We note that the foregoing argument gives us a procedure for determining all possible a-chains for a fixed value of $a \neq \pm 2$.

4. The linear recurrence relation. We shall now show that any three consecutive terms of an a-chain satisfy a linear relation.

THEOREM 2. *For any given a-chain* $\{u_i\}$ *there is a fixed integer* α *such that*

$$u_{n+1} - \alpha u_n + u_{n-1} + a = 0 \tag{5}$$

holds for any three consecutive terms of $\{u_i\}$.

Proof. Let α be the rational number such that

$$u_3 - \alpha u_2 + u_1 + a = 0.$$

We shall first show that (5) holds for all n. Since the direction of an a-chain is reversible, it is sufficient to show that (5) implies that

$$u_{n+2} - \alpha u_{n+1} + u_n + a = 0.$$

Suppose that (5) holds for a fixed n, and that u_{n+1} is not the last element of $\{u_i\}$. Then

$$\begin{aligned} u_{n+2}u_n = u_{n+1}(u_{n+1} + a) + 1 &= u_{n+1}(\alpha u_n - u_{n-1}) + 1 \\ &= \alpha u_{n+1}u_n - u_n^2 - au_n. \end{aligned}$$

Now $u_n \neq 0$, and hence

$$u_{n+2} = \alpha u_{n+1} - u_n - a,$$

which is the desired result. We need now only show that α is an integer. From (5) it follows that αu_n is an integer for all u_n. Now any two consecutive terms, u_n and u_{n+1}, are relatively prime. Hence α is an integer, and the proof of Theorem 2 is complete.

From (4) and (5) we obtain the useful identity

$$u_n^2 - \alpha u_n u_{n-1} + u_{n-1}^2 + a(u_n + u_{n-1}) + 1 = 0, \tag{6}$$

which holds for any two consecutive terms of an a-chain. Theorem 1 combined

with (6) gives us the following:

COROLLARY. *For fixed $a \neq \pm 2$ the Diophantine equation*

$$x^2 - \alpha xy + y^2 + ax + ay + 1 = 0$$

has integral solutions for only a finite number of integral values of α.

3. Explicit formulas. In this section we shall use (5) and (6) to obtain explicit formulas for the elements of the a-chain $\{u_i\}$.

Suppose first that $\alpha = -2$. Here (6) implies that

$$a = \pm 2 \text{ and } u_n + u_{n-1} = -a/2.$$

Therefore we have

$$u_{2m} = u_0, \quad u_{2m+1} = u_1, \quad u_0 + u_1 = -a/2 = \pm 1. \tag{7}$$

Thus $\{u_i\}$ is either the finite a-chain $0, -a/2, 0$ or a cyclic chain of period 2. Furthermore, if $a = \pm 2$, then (7) gives us an infinite number of a-chains. Hence Theorem 1 is false for this case.

Suppose next that $\alpha = 2$. Here the solution of (5) is

$$u_n = -an^2/2 + bn + c, \tag{8}$$

where b and c are constants which can be determined from any two terms of the a-chain.

Finally suppose that $\alpha \neq \pm 2$. We put

$$v_n = u_n - a/(\alpha - 2),$$

and (5) becomes

$$v_{n+1} - \alpha v_n + v_{n-1} = 0. \tag{9}$$

Let ξ and ξ^{-1} be the roots of

$$x^2 - \alpha x + 1 = 0.$$

Then the general solution of (9) is

$$v_n = A\xi^n + B\xi^{-n},$$

where A and B are arbitrary constants. Thus if $\alpha \neq \pm 2$ we have

$$u_n = A\xi^n + B\xi^{-n} + a/(\alpha - 2). \tag{10}$$

The constants A and B depend not only on the given a-chain but also on the particular elements chosen to be u_0 and u_1. However, if we substitute (10) in (4) and simplify, we obtain

$$AB(\alpha^2 - 4) = 1 + a^2/(\alpha - 2). \tag{11}$$

Thus the product AB depends only on a and α.

6. Positive and negative terms. To determine all positive integral solutions of the system (1), it is necessary to find all pairs of consecutive positive elements of the a-chains. We now proceed to determine the signs of the elements of all a-chains.

If $\{u_i\}$ is an a-chain, then clearly $\{-u_i\}$ is a $-a$-chain with the same value of α. Thus without loss of generality we suppose $a \geq 0$. The cases $a = 0, 1, 2$ must be discussed separately, and will be treated in later sections. Throughout this section it will be assumed that $a \geq 3$. Thus we have $u_n \neq 0$ for all n, and hence the a-chain $\{u_i\}$ has neither a first nor a last element. We begin by establishing a few simple properties, valid when $a > 2$.

I. If $\{u_i\}$ has two consecutive positive terms, then u_n is positive for all n.

II. Any negative term of $\{u_i\}$ is less than at least one of its two immediate neighbors.

Properties I and II are easy consequences of (4).

III. If $\alpha \geq -2$, and two consecutive terms of $\{u_i\}$ have opposite signs, then the positive one has smaller absolute value.

Proof. Since $\alpha \geq -2$, we have

$$u_n^2 - \alpha u_n u_{n-1} + u_{n-1}^2 \geq 0,$$

and III follows at once from (6).

IV. If $\alpha \geq -2$, then any element of $\{u_i\}$ of least absolute value is positive.

Property IV follows immediately from II and III.

It can be shown that if $a \geq 3$, the smallest possible value of α is $3 - 2a$. This value is actually assumed by the a-chain with $u_0 = u_1 = -1$. Thus

$$\alpha \geq 3 - 2a > 2 - a^2,$$

and (11) yields the result:

V. If $\alpha < -2$, then $AB < 0$.

We are now in a position to discuss the nature of the a-chains, $a \geq 3$.

Suppose first that $\alpha \geq 3$. Then u_n is given by (10), and we may suppose that $\xi > 1$. Using I, IV, and (10), we can see that either u_n is positive for all n, or $\{u_i\}$ has exactly one positive term, the term of least absolute value.

If $\alpha = 2$, then by I, IV, and (8) we see that the term of least absolute value is positive and all others are negative.

Suppose next that $|\alpha| < 2$. Then ξ is a primitive dth root of unity, where $d = 12/(3 - \alpha)$. In this case (10) can be written in the form

$$u_n = C \sin(D + 2\pi n/d) + a/(\alpha - 2),$$

where C and D are real constants. Now $a/(\alpha - 2) < 0$, and $\{u_i\}$ has at least one positive term by IV. Hence $C \neq 0$. We see that $\{u_i\}$ is cyclic of minimal period $d = 12/(3 - \alpha)$, the positive terms of $\{u_i\}$ are those of least absolute value, and there is only one positive term in each cycle.

Since $\alpha = -2$ is possible only if $a = \pm 2$, we need now only consider $\alpha \leq -3$.

If $\alpha \leq -3$ we may assume that $-1 < \xi < 0$. By replacing, if necessary, u_n by u_{n-1} in (10), we may suppose also that $A < 0$. Then by V, $B > 0$. Hence

$$u_{2m+2} > u_{2m} \quad \text{and} \quad u_{2m+1} < u_{2m-1}$$

for all integral m. Furthermore, for m sufficiently large, u_{2m} and u_{-2m-1} are positive while u_{2m+1} and u_{-2m} are negative. It follows from I and II that $\{u_i\}$ has no consecutive positive terms and exactly one pair of consecutive negative terms.

Since all $-a$-chains can be obtained by reversing the signs of a-chains, similar results hold for $a \leq -3$.

7. The case $a = 2$. Let us suppose first that $\{u_i\}$ is a 2-chain with at least one zero element, say $u_0 = 0$. Without loss of generality we can suppose that u_0 is the first term of $\{u_i\}$. Then (4) yields $u_1 = -1$. It is easily seen that $0, -1, u_2, \cdots$ is a 2-chain for any integral value of u_2, and that $\alpha = -u_2 - 2$. If $u_2 \leq -4$, then it follows from (8) and (10) that $u_n < 0$ for all $n > 0$. If $-3 \leq u_2 \leq 0$ then $\{u_i\}$ has finite length and no positive terms. If $u_2 > 0$, then it can be shown

that u_n and u_{n+1} have opposite signs for all $n > 0$.

We may now assume that $\{u_i\}$ is a 2-chain with no zero terms. Since

$$(u_n + 1)^2 = u_{n-1}\, u_{n+1} \neq 0,$$

we see that $u_n \neq -1$ for all n. We suppose next that there is an i such that $u_i = 1$, say $u_1 = 1$. Then $u_0\, u_2 = 4$. Without loss of generality we can take $u_2 \geq u_0$ and thus $u_2 = 4$, 2, or -2. Putting $u_2 = 4$, we obtain the 2-chain $\cdots$, 25, 4, 1, 1, 4, 25, $\cdots$ with $\alpha = 7$, whose terms are the squares of alternate elements of the Fibonacci sequence[1]. Putting $u_2 = 2$, we obtain the 2-chain $\cdots$, 9, 2, 1, 2, 9, 50, $\cdots$ with $\alpha = 6$. The odd terms of this 2-chain are perfect squares, and the even terms are of the form $2N^2$. If we put $u_2 = -2$, we get the 2-chain $\cdots, -2$, 1, -2, 1, $\cdots$, which is a member of the infinite family of cyclic chains defined by (7).

We suppose finally that $\{u_i\}$ is a 2-chain with all $|u_n| > 1$, and that u_1 is a term of least absolute value. Now u_0 and u_2 are both relatively prime to u_1, and hence

$$|u_0| > |u_1|, \quad |u_2| > |u_1|.$$

Therefore

$$(u_1 + 1)^2 = u_0\, u_2 > u_1^2.$$

Thus

$$u_1 > 0 \text{ and } u_2 = u_0 = \pm(u_1 + 1).$$

Now if $u_2 = -u_1 - 1$, then $\alpha = -2$, and we are led to the infinite family of 2-chains given by (7). If $u_2 = u_1 + 1$, then we have

$$u_1 \mid (u_2 + 1)^2 = (u_1 + 2)^2.$$

Therefore u_1 is either 2 or 4, and we are led to the two 2-chains: $\cdots$, 3, 2, 3, 8, $\cdots$ with $\alpha = 4$, and $\cdots$, 5, 4, 5, 9, $\cdots$ with $\alpha = 3$. Thus every 2-chain falls into one of three classes:

(A) an infinite class of chains with at least one zero term, one chain for each value of α;

---

[1] The Fibonacci sequence 1, 1, 2, 3, 5, 8, $\cdots$ is defined by $U_0 = U_1 = 1$ and $U_{n+1} = U_n + U_{n-1}$.

(B) an infinite class of cyclic chains with period 2, $\alpha = -2$, and no zero terms;

(C) four special chains with all positive terms and $\alpha = 3$, 4, 6, and 7 respectively.

We can obtain all -2-chains by reversing the signs of these 2-chains.

8. The case $a = 1$. Here $u_n \neq 0$ for all n. Without loss of generality we suppose that u_1 has least absolute value, and that $|u_2| \geq |u_0|$. Since

$$|u_0 u_2| = |u_1^2 + u_1 + 1| < (|u_1| + 1)^2,$$

it follows that $|u_0| = |u_1|$. Since u_0 and u_1 are relatively prime, it follows that $u_1 = \pm 1$. Suppose first that $u_1 = 1$. Then $u_0 u_2 = 3$. Hence $u_2 = \pm 3$. If $u_2 = 3$ then we have the 1-chain[2]

$$\cdots, 13, 3, 1, 1, 3, 13, 61, 291, 1393, \cdots$$

with $\alpha = 5$. If $u_2 = -3$, we have the 1-chain $\cdots, 1, -1, 1, -3, 7, \cdots$ with $\alpha = -3$. We suppose next that $u_1 = -1$. Here $u_0 u_2 = 1$. If we put $u_2 = 1$, we obtain the last mentioned 1-chain again. If $u_2 = -1$, then $u_n = -1$ for all n, and we have the constant 1-chain $\cdots, -1, -1, -1, \cdots$ with $\alpha = 1$.

Thus we see that there are exactly three 1-chains, one consisting entirely of positive terms, one in which every term is -1, and one consisting of alternating positive and negative terms. We have proved the following theorem.

THEOREM 3. *Let x and y be positive integers. Then*

$$x \mid y^2 + y + 1 \text{ and } y \mid x^2 + x + 1$$

if and only if x and y are consecutive terms of the sequence 1, 1, 3, 13, $\cdots$, *where the nth term is given by*

$$u_n = 5u_{n-1} - u_{n-2} - 1.$$

Furthermore,

$$x \mid y^2 - y + 1 \text{ and } y \mid x^2 - x + 1$$

if and only if $x = y = 1$.

9. The case $a = 0$. As in the previous section, we suppose $|u_1|$ minimal and

[2] The accidental discovery of the relations $13 \mid 61^2 + 61 + 1$ and $61 \mid 13^2 + 13 + 1$ led to this entire investigation.

$|u_2| \geq |u_0|$. We note that if the integers u_n form a 0-chain then so do the integers $-u_n$ and the integers $(-1)^n u_n$. Thus it is sufficient to consider the case where $u_1 > 0$ and $u_2 > 0$. Now u_0 and u_2 are both relatively prime to u_1, and hence if $u_1 > 1$ we have

$$|u_0 u_2| \geq (u_1 + 1)^2 > u_1^2 + 1 = |u_0 u_2|.$$

Therefore

$$u_1 = 1, \quad u_0 u_2 = 2, \quad \text{and hence} \quad u_2 = 2, \quad u_0 = 1.$$

This leads us to the 0-chain $\cdots, 5, 2, 1, 1, 2, 5, 13, \cdots$ with $\alpha = 3$. We note that the elements of this 0-chain are alternate elements of the Fibonacci sequence. We see that there are exactly three 0-chains, one consisting entirely of positive terms, one consisting entirely of negative terms, and one with alternately positive and negative terms. Furthermore, we have proved the following theorem.

THEOREM 4. *Let x and y be positive integers. Then*

$$x \mid y^2 + 1 \quad \text{and} \quad y \mid x^2 + 1$$

if and only if x and y are consecutive elements in the sequence 1, 1, 2, 5, 13, $\cdots$ *whose elements are alternate terms of the Fibonacci sequence.*

10. Table of a-chains, $0 \leq a \leq 10$. By methods similar to those used in the last three sections, it is a simple matter to determine all a-chains for small positive values of a. In the table on page 123 we give the values of a and α, and three consecutive terms of each a-chain, $0 \leq a \leq 10$. In the table, u stands for an arbitrary integer and r for an arbitrary positive integer.

11. Systems with a finite number of solutions. If $a \geq 0$, then the a-chain $\cdots, 1, 1, a+2, \cdots$ leads to an infinite number of positive integral solutions of the original system (1), and $\cdots, -1, 1, -a-2, \cdots$ leads to an infinite number of positive solutions of the system

$$x \mid y^2 + ay + 1, \quad y \mid x^2 - ax + 1.$$

On the other hand, there are values of a for which the system

$$x \mid y^2 - ay + 1, \quad y \mid x^2 - ax + 1 \tag{12}$$

has only a finite number of positive integral solutions. Using the results of § 6,

TABLE OF a-CHAINS, $0 \leq a \leq 10$.

a	α	u_0,	u_1,	u_2
0	-3	-1,	1,	-2
	3	-1,	-1,	-2
	3	1,	1,	2
1	-3	-1,	1,	-3
	1	-1,	-1,	-1
	5	1,	1,	3
2	$-u-2$	0,	-1,	u
	-2	$-1-r$,	r,	$-1-r$
	3	5,	4,	5
	4	3,	2,	3
	6	2,	1,	2
	7	1,	1,	4
3	-3	-1,	-1,	1
	9	1,	1,	5
4	-5	-1,	-1,	2
	-3	-2,	-1,	1
	-1	-2,	1,	-3
	9	2,	1,	3
	11	1,	1,	6
5	-7	-1,	-1,	3
	-3	-3,	-1,	1
	5	5,	3,	5
	13	1,	1,	7
6	-9	-1,	-1,	4
	-6	-2,	-1,	2
	-3	-4,	-1,	1
	0	-2,	1,	-4
	12	2,	1,	4
	15	1,	1,	8
7	-11	-1,	-1,	5
7	-3	-5,	-1,	1
	1	-3,	1,	-3
	13	3,	1,	3
	17	1,	1,	9
8	-13	-1,	-1,	6
	-9	-2,	-1,	3
	-7	-3,	-1,	2
	-3	-6,	-1,	1
	-1	-3,	2,	-7
	1	-2,	1,	-5
	5	6,	5,	11
	9	3,	2,	7
	15	2,	1,	5
	19	1,	1,	10
9	-15	-1,	-1,	7
	-3	-7,	-1,	1
	21	1,	1,	11
10	-17	-1,	-1,	8
	-12	-2,	-1,	4
	-8	-4,	-1,	2
	-6	-3,	-2,	5
	-4	-5,	-2,	3
	-3	-5,	-3,	4
	-3	-8,	-1,	1
	-1	-5,	3,	-8
	0	-5,	2,	-5
	2	-2,	1,	-6
	3	-3,	1,	-4
	3	23,	19,	24
	8	4,	3,	10
	10	5,	2,	5
	17	3,	1,	4
	18	2,	1,	6
	23	1,	1,	12

we see that (12) has an infinite number of positive integral solutions if and only if there exists an a-chain with $\alpha > 1$ which has at least one negative term.

If $a > 8$, then a necessary condition that (12) have only a finite number of positive integral solutions is that $a + 2$ be prime. For if $a + 2 = RS$, $a > 8$, $R > 1$, $S > 1$, then $\cdots, -R, 1, -S, \cdots$ is an a-chain with $\alpha > 1$. This condition is not sufficient, for $\cdots, -7, 3, -19, \cdots$ is a 41-chain with $\alpha = 5$.

Futhermore, if $a = 1$ or if $3 \leq a \leq 9$, then (12) has only a finite number of positive solutions. For example, the system

$$x \mid y^2 - 8y + 1, \quad y \mid x^2 - 8x + 1, \quad y \geq x > 0$$

has exactly nine integral solutions, namely $x = 1$, $y = 1$, 2, 3, and 6; $x = 2$, $y = 11$; $x = 3$, $y = 7$; $x = 5$, $y = 14$; $x = 11$, $y = 17$; and $x = 14$, $y = 17$.

YALE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

Vari-Type Composition by
Elaine Barth
Delores Wierman

With the cooperation of
E. F. Beckenbach
E. G. Straus

Printed in the United States of America by
Edwards Brothers, Inc., Ann Arbor, Michigan

UNIVERSITY OF CALIFORNIA PRESS * BERKELEY AND LOS ANGELES

Pacific Journal of Mathematics
Vol. 3, No. 1 March, 1953