THREE DIOPHANTINE EQUATIONS – PART I

IRVING ADLER
North Bennington, Vermont

1. INTRODUCTION

This article deals with the three Diophantine equations

$$x^2 + (x + 1)^2 = z^2 \tag{1}$$

$$u^2 + u = 2v^2 \tag{2}$$

$$s^2 + 2t^2 = 1 \ . \tag{3}$$

These equations have been studied by various methods for hundreds of years, and their solutions in positive integers are well known. (See the historical note at the end of Part II, Feb.) However, as often happens with old problems, people not aware of the long history of these equations keep rediscovering them and their solutions. An article recently submitted to the Fibonacci Quarterly dealt with Eq. (1), and solved it by transforming it into Eq. (3). Elementary Problem B-102 in the December 1966 issue of the Quarterly (page 373) also links Eq. (1) and the solution to Eq. (3). Another article recently submitted to the Quarterly deals with Eq. (2).

The three equations are essentially equivalent because, as we shall see in Section 9, each can be transformed into each of the other two by a linear transformation.

2. WHY THE EQUATIONS KEEP COMING UP

The equations come up over and over again because they arise in a natural way from some basic problems of number theory.

A. When the general solution of the equation $x^2 + y^2 = z^2$ is studied, it is natural to consider the special case in which x and y are consecutive integers. This leads to Eq. (1).

B. When people play with figurate numbers, and, in particular, with the triangular numbers

$$T(u) = \tfrac{1}{2}u(u + 1) \quad ,$$

and the square numbers

$$S(v) = v^2 \quad ,$$

they soon observe that

$$36 = S(6) = T(8) \quad .$$

This observation naturally suggests the problem of finding all the triangular numbers that are also square numbers. This problem leads to Eq. (2).

C. There is no rational number s/t equal to the square root of 2. That is, there are no positive integers s and t such that

$$s^2 - 2t^2 = 0 \quad . \tag{4}$$

However, it is possible to obtain rational approximations to the square root of 2 with errors smaller than any prescribed amount. The search for rational approximations with a small error naturally leads to consideration of the equation obtained from Eq. (4) by requiring the right-hand member to be 1 instead of 0. This leads to Eq. (3).

3. SOLUTIONS BY TRIAL AND ERROR

One way of finding some positive integers that satisfy Eq. (1) is to substitute first 1, then 2, etc., for x in the expression $x^2 + (x + 1)^2$ to identify values of x which make the expression a perfect square. Similarly, solutions of Eq. (2) can be found by identifying by trial and error some positive integral values of u that make

$$\tfrac{1}{2}u(u + 1)$$

a perfect square. And solutions of Eq. (3) can be found by identifying some positive integral values of t that make $1 + 2t^2$ a perfect square. Anyone with patience and a table of squares, or who has access to a computer can discover in this way at least a few of the solutions of each of the three equations.

It will be useful to us to identify not only positive solutions, but non-negative solutions. The first five non-negative solutions of Eqs. (1), (2), and (3) are shown in the table below:

Solutions of Equation (1)

x	z
0	1
3	5
20	29
119	169
696	985

Solutions of Equation (2)

u	v
0	0
1	1
8	6
49	35
288	204

Solutions of Equation (3)

s	t
1	0
3	2
17	12
99	70
577	408

4. CAN WE COMPUTE MORE SOLUTIONS FROM THOSE WE ALREADY HAVE?

Once we have the first few solutions of one of these equations, we may, by inspecting them, find a relationship by which more solutions can be calculated. To facilitate the formulation of such a relationship, let us index the solutions of each equation in order of magnitude, with the non-negative integers 0, 1, 2, $\cdots$, respectively, used as indices. Then, in this notation,

$$x_0 = 0, \quad z_0 = 1, \quad x_1 = 3, \quad z_1 = 5, \quad x_2 = 20, \quad z_2 = 29,$$

etc. Are there, perhaps, formulas that permit us to calculate x_n and z_n in terms of x_{n-1} and z_{n-1}? Let us assume there are such formulas, and let us guess that they are linear. Assume that

$$x_n = ax_{n-1} + bz_{n-1} + c \,, \tag{5}$$

$$z_n = dx_{n-1} + ez_{n-1} + f \,. \tag{6}$$

Then we have to use only the first four values of x and z to determine what the values of a, b, c, d, e and f must be. Taking n equal to 1, 2, and 3 in succession, we get the following systems of equations:

$$\begin{cases} 3 = a \cdot 0 + b \cdot 1 + c \\ 20 = a \cdot 3 + b \cdot 5 + c \\ 119 = a \cdot 20 + b \cdot 29 + c\ , \end{cases} \qquad \begin{cases} 5 = d \cdot 0 + e \cdot 1 + f \\ 29 = d \cdot 3 + e \cdot 5 + f \\ 169 = d \cdot 20 + e \cdot 29 + f\ . \end{cases}$$

Solving these systems of equations, we find that

$$a = 3, \quad b = 2, \quad c = 1, \quad d = 4, \quad e = 3, \quad \text{and} \quad f = 2\ .$$

Equations (5) and (6) are merely guesses. However, the fact that the values of a, b, c, d, e and f that we calculated on the basis of these guesses turns out to be integers, and small ones, at that, is presumptive evidence in favor of these guesses. Let us continue operating with these guesses. If Eqs. (5) and (6) are true, then they must take this form:

$$x_n = 3x_{n-1} + 2z_{n-1} + 1\ , \tag{7}$$

$$z_n = 4x_{n-1} + 3z_{n-1} + 2\ . \tag{8}$$

We can obtain more evidence for or against our guesses by using Eqs. (7) and (8) to calculate x_4 and z_4:

$$x_4 = 3(119) + 2(169) + 1 = 696\ ;$$
$$z_4 = 4(119) + 3(169) + 2 = 985\ .$$

Since these values of x_4 and z_4 calculated by means of Eqs. (7) and (8) agree with the values of x_4 and z_4 in the table, the evidence tends to support the correctness of Eqs. (7) and (8). We now know that Eqs. (7) and (8) are true when n = 1, 2, 3, or 4. This gives us the confidence to seek a proof that they are true for all positive integral values of n. The proof is given in the next section.

EXERCISES

1. Let (u_n, v_n) be the n^{th} positive integral solution of Eq. (2). If we assume that

$$u_n = au_{n-1} + bv_{n-1} + c ,$$

and

$$v_n = du_{n-1} + ev_{n-1} + f ,$$

then what values must a, b, c, d, e and f have in these formulas?

2. Let (S_n, t_n) be the n^{th} solution in positive integers of Eq. (3). If we assume that

$$s_n = as_{n-1} + bt_{n-1} + c ,$$

and

$$t_n = ds_{n-1} + et_{n-1} + f ,$$

then what values must a, b, c, d, e and f have in these formulas?

5. PROOF THAT SUCCESSIVE SOLUTIONS ARE LINEARLY RELATED

The preceding section led to the conjecture that successive solutions of Eq. (1) are related by the linear Eqs. (7) and (8). To prove the conjecture, it is necessary to show that

A. If (x_{n-1}, z_{n-1}) is a solution of Eq. (1), then (x_n, z_n) defined by Eqs. (7) and (8) is also a solution;

B. If we take $x_0 = 0$ and $z_0 = 1$, then every solution of Eq. (1) can be obtained by starting with (x_0, z_0) and making repeated use of Eqs. (7) and (8), to generate solutions with greater and greater values of x and z.*

Proof of A. Suppose that (x_{n-1}, z_{n-1}) is a solution of Eq. (1). Then we want to show that

$$(3x_{n-1} + 2z_{n-1} + 1, \quad 4x_{n-1} + 3z_{n-1} + 2)$$

*The proof given here is adapted from that given in [1].

is also a solution of Eq. (1). To simplify the notation for the proof, let us drop the subscripts. In this simplified notation, we are assuming that

$$x^2 + (x + 1)^2 = z^2 ,$$

and we want to show that

$$(3x + 2z + 1)^2 + (3x + 2z + 2)^2 = (4x + 3z + 2)^2 .$$

$$\begin{aligned}(3x + 2z + 1)^2 + (3x + 2z + 2)^2 \\ &= 18x^2 + 24xz + 8z^2 + 18x + 12z + 5 \\ &= 16x^2 + 24xz + 8z^2 + 16x + 12z + 4 + (2x^2 + 2x + 1) \\ &= 16x^2 + 24xz + 9z^2 + 16x + 12z + 4 \\ &= (4x + 3z + 2)^2 .\end{aligned}$$

in view of the fact that

$$2x^2 + 2x + 1 = x^2 + (x + 1)^2 = z^2 .$$

Proof of B. Equations (7) and (8) determine a function

$$f : (x, z) \longrightarrow (x', z')$$

as follows:

$$\text{(f)} \qquad \begin{cases} x' = 3x + 2z + 1 , \\ z' = 4x + 3z + 2 . \end{cases}$$

If we solve these equations for x and z, we obtain the inverse function

$$\text{(g)} \qquad (x', z') \longrightarrow (x, z)$$

defined by

$$(10)\qquad \begin{cases} x = 3x' - 2z' + 1, \\ z = -4x' + 3z' - 2. \end{cases}$$

$fg = i =$ the identity function. Then

$$ffgg = f(fg)g = fig = fg = i,$$

and, in general,

$$f^n g^n = i$$

for every positive integer n. That is,

$$f^n g^n (x, z) = (x, z).$$

We shall show first that if (x, z) is a solution of Eq. (1), with $x > 0$, $z > 0$, then

$$(x_1, z_1) = g(x, z)$$

is a solution of Eq. (1) with $x_1 \geq 0$, and $z_1 > 0$, and $z_1 < z$. If

$$x^2 + (x+1)^2 = z^2,$$

then

$$\begin{aligned} x_1^2 + (x_1+1)^2 &= 2x_1^2 + 2x_1 + 1 = 2(3x - 2z + 1)^2 + 2(3x - 2z + 1) + 1 \\ &= 18x^2 + 8z^2 - 24xz + 18x - 12z + 5 \\ &= 16x^2 + 8z^2 - 24xz + 16x - 12z + 4 + (2x^2 + 2x + 1) \\ &= 16x^2 + 9z^2 - 24xz + 16x - 12z + 4, \end{aligned}$$

since

$$2x^2 + 2x + 1 = x^2 + (x + 1)^2 = z^2 ,$$

then

$$x_1^2 + (x_1 + 1)^2 = (-4x + 3z - 2)^2 = z_1^2 .$$

Therefore (x_1, z_1) is a solution of Eq. (1). Now we aim to show that $x_1 \geq 0$, $z_1 > 0$, and $z_1 < z$. The condition $x_1 \geq 0$ is equivalent to $3x - 2z + 1 \geq 0$. or $2z \leq 3x + 1$. The condition that $z_1 > 0$ is equivalent to $-4x + 3x - 2 > 0$, or $3z > 4x + 2$. The condition $z_1 < z$ is equivalent to $-4x + 3z - 2 < z$, or $z < 2x + 1$. So we shall show that

$$z < 2x + 1, \quad 2z \leq 3x + 1 ,$$

and

$$3z > 4x + 2 .$$

$$z^2 = 2x^2 + 2x + 1 = 4x^2 + 4x + 1 - 2x^2 - 2x$$
$$= (2x + 1)^2 - 2x(x + 1) < (2x + 1)^2 ,$$

since $x > 0$, and hence $2x(x + 1) > 0$. Therefore $z < 2x + 1$. Since

$$z^2 = 2x^2 + 2x + 1 ,$$

and $x > 0$, then

$$9z^2 = 18x^2 + 18x + 9 > 16x^2 + 16x + 4 = (4x + 2)^2 .$$

Therefore $3z > 4x + 2$.

$$4z^2 = 8x^2 + 8z + 4 = 9x^2 + 6x + 1 - x^2 + 2x + 3 .$$

Since $x > 0$, we see from the table of solutions of Eq. (1) that $x \geq 3$. Then

$$x^2 \geq 3x = 2x + x \geq 2x + 3 .$$

Then

$$2x + 3 - x^2 \leq 0 .$$

Consequently

$$4z^2 \leq 9x^2 + 6x + 1 = (3x + 1)^2 ,$$

and

$$2z \leq 3x + 1 .$$

We have shown that if (x, z) is a solution of Eq. (1) for which $x > 0$ and $z > 0$, then

$$(x_1, z_1) = g(x, z)$$

is a solution for which $x_1 \geq 0$, $z_1 > 0$, and $z_1 > z$. If $x_1 > 0$ we can repeat the process to obtain a solution

$$(x_2, z_2) = g(x_1, z_1) = g^2(x, z) ,$$

with $x_2 \geq 0$, $z_2 > 0$, and $z_2 < z_1$. Continuing in this way as long as $x_i > 0$, $i = 1, 2, \cdots$, we get a descending sequence of positive integers $z > z_1 > z_2 > \cdots$. Since this sequence must terminate, there exists a positive integer n for which

$$(x_n, z_n) = g^n(x, z)$$

is a solution of Eq. (1) with $x_n = 0$. Then $z_n = 1$, and

$$(0, 1) = (x_n, z_n) = g^n(x, z) .$$

Then

$$f^n(0, 1) = f^n g^n(x, z) = (x, z) .$$

This completes the proof of Part B.

If we return now to the notation of Eqs. (7) and (8), we can say that all solutions of Eq. (1) are given by the formula

$$(x_n, z_n) = f^n(0, 1), \quad n = 1, 2, 3, \cdots \tag{11}$$

where f is defined by (9).

EXERCISES

3. Exercise 1 leads to the conjecture that successive solutions of Eq. (2) are related by the equations

$$u_n = 3u_{n-1} + 4v_{n-1} + 1 , \tag{12}$$

$$v_n = 2u_{n-1} + 3v_{n-1} + 1 . \tag{13}$$

Let the function g be defined by

$$g(u, v) = (3u + 4v + 1, \quad 2u + 3v + 1) .$$

Using the method employed above, prove that all solutions in positive integers in Eq. (2) are given by

$$(u_n, v_n) = g^n(0, 0), \quad n = 1, 2, 3, \cdots \tag{14}$$

4. Exercise 2 leads us to the conjecture that successive solutions of Eq. (3) are related by the equations

$$s_n = 3s_{n-1} + 4t_{n-1} , \tag{15}$$

$$t_n = 2s_{n-1} + 3t_{n-1} . \tag{16}$$

(Continued on p. 317.)