GENERATING SOLUTIONS FOR A SPECIAL CLASS OF DIOPHANTINE EQUATIONS

Pasquale J. Arpaia
Department of Mathematics and Computer Science, St. John Fisher College, Rochester, NY 14618
(Submitted August 1992)

Let $p = p(x_1, x_2, \ldots, x_n)$ be a polynomial with positive integer coefficients. In this paper we shall discuss some methods for generating solutions for the equation

$$p + y^2 = z^2. \tag{1}$$

The approach we use is to start with a method for generating solutions for the equaiton

$$x^2 + y^2 = z^2, \tag{2}$$

and show how the method is extended to equation (1) or to special cases of (1).

1. THE RULE OF PYTHAGORAS AND THE RULE OF PLATO

According to Dickson [1], it was Pythagoras who showed that, if we start with the odd integer a, let $b = \frac{1}{2}(a^2 - 1)$ and $c = b + 1$, then (a, b, c) is a solution of (2).

Again, according to Dickson [1], it was Plato who showed that, if we start with the even integer a, let $b = \frac{1}{4}a^2 - 1$ and $c = b + 2$, then (a, b, c) is also a solution of (2).

The methods of Pythagoras and Plato are extended to (1) by the following proposition.

Proposition 1: Let $a_1, a_2, \ldots, a_n$ be positive integers and let $a = p(a_1, a_2, \ldots, a_n)$.

i. If a is odd, let $b = \frac{1}{2}(a - 1)$ and $c = b + 1$, then $(a_1, a_2, \ldots, a_n, b, c)$ is a solution of (1).

ii. If $a \equiv 0 \pmod 4$, let $b = \frac{1}{4}a - 1$ and $c = b + 2$, then $(a_1, a_2, \ldots, a_n, b, c)$ is a solution of (1).

iii. If $a \equiv 2 \pmod 4$, then it is impossible to find integers b and c such that $(a_1, a_2, \ldots, a_n, b, c)$ is a solution of (1).

Proof: For i and ii, write $c^2 - b^2$ as $(c - b)(c + b)$, substitute and simplify. If $a \equiv 2 \pmod 4$, then, for integers b and c, $a + b^2 \equiv 2$ or $3 \pmod 4$ depending on whether b is even or odd, respectively, but $c^2 \equiv 0$ or $1 \pmod 4$ depending on whether c is even or odd, respectively.

2. THE METHOD OF RECURSION

Let (a, b, c) be a solution of (2). Let $d = c - b$, $a_1 = a + d$, $b_1 = a + b + \frac{d}{2}$, and $c_1 = b_1 + d$ In [2] I showed that (a_1, b_1, c_1) is also a solution of (2). Let us call this method the "method of recursion." The following proposition extends the method of recursion to the equation

$$k_1x_1^2 + k_2x_2^2 + \cdots + k_nx_n^2 + m + y^2 = z^2. \tag{3}$$

Proposition 2: Let $(a_1, a_2, \ldots, a_n, b, c)$ be a solution of equation (3) and let $d = c - b$. For $i = 1$ to n define

$$a_i' = a_i + d,\ b' = \Sigma k_i a_i + b + \frac{d\Sigma k_i}{2},\ \text{and}\ c' = b' + d.$$

Then $(a_1', a_2', \ldots, a_n', b', c')$ is also a solution of (3).

Proof: Substitute $a_i + d$ for a_i' and simplify to obtain

$$\Sigma k_i (a_i')^2 = \Sigma k_i (a_i + d)^2 = \Sigma k_i a_i^2 + 2d\Sigma k_i a_i + d^2 \Sigma k_i.$$

Substitute $c^2 - b^2 - m$ for $\Sigma k_i a_i^2$, write $c^2 - b^2$ as $d(c+b)$, and factor out d to obtain

$$d(c + b + 2\Sigma k_i a_i + d\Sigma k_i) - m.$$

Substitute $2b' - 2b$ for $2\Sigma k_i a_i + d\Sigma k_i$ to obtain

$$d(c + b + 2\Sigma k_i a_i + d\Sigma k_i) - m = d(c - b + 2b') - m.$$

And since $c - b = c' - b' = d$, we obtain

$$d(c - b + 2b') - m = (c')^2 - (b')^2 - m.$$

Note that when $d\Sigma k_i$ is odd we do not obtain integer solutions (see Example 1 below). In this case, apply the recursion twice to obtain the following corollary.

Corollary Let $(a_1, a_2, \ldots, a_n, b, c)$ be a solution of equation (3) and let $d = c - b$. For $i = 1$ to n define

$$a_i' = a_i + 2d,\ b' = 2\Sigma k_i (a_i + d) + b,\ \text{and}\ c' = b' + d.$$

Then $(a_1', a_2', \ldots, a_n', b', c')$ is also a solution of (3).

The following example illustrates the use of Proposition 1, Proposition 2, and its Corollary.

Example 1: Suppose we begin with the equation

$$2x_1^2 + x_2^2 + 2x_3^2 + 4 + y^2 = z^2. \tag{4}$$

If we let $x_1 = x_3 = 1$ and $x_2 = 2$, then, by Proposition 1, (1, 2, 1, 2, 4) is a solution of (4). Here, $d = 4 - 2 = 2$. Applying Proposition 2, we have

$$\begin{aligned} &a_1' = 3,\ \ a_2' = 4,\ \ a_3' = 3, \\ &b' = 2\cdot 1 + 1\cdot 2 + 2\cdot 1 + 2 + \frac{2(2+1+2)}{2} = 13, \\ &c' = 15. \end{aligned}$$

Hence, (3, 4, 3, 13, 15) is also a solution of (4).

If we let $x_1 = x_2 = x_3 = 1$, then, by Proposition 1, (1, 1, 1, 4, 5) is a solution of (4). Here, $d = 5 - 4 = 1$. Applying Proposition 2, we have

$$\begin{aligned} &a_i' = 2,\ \ a_2' = 2,\ \ a_3' = 2, \\ &b' = 2\cdot 1 + 1\cdot 1 + 2\cdot 1 + 4 + \frac{(2+1+2)}{2} = \frac{23}{2}, \\ &c' = \frac{25}{2}. \end{aligned}$$

Hence, $\left(2, 2, 2, \frac{23}{2}, \frac{25}{2}\right)$ is also a solution of (4).

In this case, the solution is not an integer solution. However, if we apply the Corollary to Proposition 2, we obtain

$$a_1' = 3,\ \ a_2' = 3,\ \ a_3' = 3,$$
$$b' = 2(2\cdot 2 + 1\cdot 2 + 2\cdot 2) + 4 = 24,$$
$$c' = 25.$$

Hence, (3, 3, 3, 24, 25) is also a solution of (4).

3. THE METHOD OF MATRICES

In [3], Hall showed that, if we mutliply a solution (a, b, c) of (2) by any of the following three matrices, the product is also a solution of (2).

$$\begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$$

Let us call this method the "method of matrices." The following proposition extends the method of matrices to the equation

$$nx^2 + y^2 + m = z^2. \tag{5}$$

Proposition 3: Let (a, b, c) be a solution of equation (5).

i. If $n = 2k$, the product of (a, b, c) and any of the following three matrices is also a solution of (5).

$$\begin{bmatrix} 1 & -1 & 1 \\ 2k & 1-k & k \\ 2k & -k & k+1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 \\ 2k & k-1 & k \\ 2k & k & k+1 \end{bmatrix} \quad \begin{bmatrix} -1 & 1 & 1 \\ -2k & k-1 & k \\ -2k & k & k+1 \end{bmatrix}$$

ii. If $n = 2k+1$, the product of (a, b, c) and any of the following three matrices is also a solution of (5)

$$\begin{bmatrix} 1 & -2 & 2 \\ 2n & 1-2n & 2n \\ 2n & -2n & 2n+1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 2 \\ 2n & 2n-1 & 2n \\ 2n & 2n & 2n+1 \end{bmatrix} \quad \begin{bmatrix} -1 & 2 & 2 \\ -2n & 2n-1 & 2n \\ -2n & 2n & 2n+1 \end{bmatrix}$$

(Note that when $n = 1$ we obtain Hall's matrices stated above.)

Proof: Equation (5) is a special case of equation (3). By Proposition 2, with $k_1 = n$,

$$a' = a + d,\ \ b' = na + b + \frac{nd}{2},\ \text{ and }\ c' = b' + d,$$

is also solution of (5). Let $n = 2k$, substitute $c - b$ for d, and simplify to obtain

$$a' = a - b + c,$$
$$b' = 2ka + (1-k)b + kc,$$
$$c' = 2ka - kb + (k+1)c.$$

In matrix form, this becomes

$$\begin{bmatrix} 1 & -1 & 1 \\ 2k & 1-k & k \\ 2k & -k & k+1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

To obtain the second matrix, note that, if (a, b, c) is a solution, then so is $(a, -b, c)$. Hence

$$\begin{bmatrix} 1 & -1 & 1 \\ 2k & 1-k & k \\ 2k & -k & k+1 \end{bmatrix} \begin{bmatrix} a \\ -b \\ c \end{bmatrix}$$

is also a solution. But

$$\begin{bmatrix} 1 & -1 & 1 \\ 2k & 1-k & k \\ 2k & -k & k+1 \end{bmatrix} \begin{bmatrix} a \\ -b \\ c \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 \\ 2k & 1-k & k \\ 2k & -k & k+1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

The third matrix is obtained similarly.

When $n = 2k+1$, we use the Corollary to Proposition 2.

The following example illustrates the use of Proposition 1 and Proposition 3.

Example 2: Suppose we begin with the equation

$$2x^2 + y^2 = z^2. \tag{6}$$

By Proposition 1, (2, 1, 3) is a solution of equation (6). Since n is even, by Proposition 3 the matrices

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & 0 & 1 \\ 2 & -1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 \\ 2 & 0 & 1 \\ 2 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} -1 & 1 & 1 \\ -2 & 0 & 1 \\ -2 & 1 & 2 \end{bmatrix}$$

and the triple (2, 1, 3) will generate the solutions (4, 7, 9), (6, 7, 11), and (2, -1, 3), respectively.

If we begin with the equation

$$3x^2 + y^2 = z^2, \tag{7}$$

then, by Proposition 1, (1, 1, 2) is a solution of equation (7). Since n is odd, by Proposition (3) the matrices

$$\begin{bmatrix} 1 & -2 & 2 \\ 6 & -5 & 6 \\ 6 & -6 & 7 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 2 \\ 6 & 5 & 6 \\ 6 & 6 & 7 \end{bmatrix} \quad \begin{bmatrix} -1 & 2 & 2 \\ -6 & 5 & 6 \\ -6 & 6 & 7 \end{bmatrix}$$

and the triple (1, 1, 2) will generate the solutions (3, 13, 14), (7, 23, 26), and (5, 11, 14), respectively.

REFERENCES

1. L. E. Dickson. *History of the Theory of Numbers.* Vol. II. New York: Chelsea, 1966.
2. P. J. Arpaia. "A Generating Property of Pythagorean Triples." *Math. Magazine* **44.1** (1971).
3. A. Hall. "Genealogy of Pythagorean Triads." *London Mathematical Gazette* **59.387** (1970).

AMS Classification Number: 11B39

❖❖❖