APPLICATION OF RECURSIVE SEQUENCES TO DIOPHANTINE EQUATIONS

RAPHAEL FINKELSTEIN
Bowling Green State University, Bowling Green, Ohio
EDGAR KARST
University of Arizona, Tuscon, Arizona
HYMIE LONDON
McGill University, Montreal, Canada

ABSTRACT

In a former version of this paper ("Iteration Algorithms for Certain Sums of Squares"), Karst, by composition of simple sums of squares, found six iteration algorithms of which he could prove the first by means of the generalized Pell equation and the second by the permanence of formal laws. For the remaining four, equivalent to the solution of $x^2 - (k^2+1)y^2 = k^2$, with $k = 1, 2,$ and 3, Finkelstein and London were able to furnish a unifying proof by the use of class numbers and quadratic fields. This justifies the new title.

The following three-step iteration algorithm to generate x in $2x + 1 = a^2$ and $3x + 1 = b^2$, simultaneously, was mentioned in [6, p. 211]:

$1 \cdot 10 - 1 = 9$	$9^2 = 81$	$(81-1)/2 = 40 = x_1$
$9 \cdot 10 - 1 = 89$	$89^2 = 7921$	$(7921-1)/2 = 3960 = x_2$
$89 \cdot 10 - 9 = 881$	$881^2 = 776161$	$(776161-1)/2 = 388080 = x_3$
$881 \cdot 10 - 89 = 8721$	$8721^2 = 765055841$	$(76055841-1)/2 = 38027920 = x_4$
$8721 \cdot 10 - 881 = 86329$	$86329^2 = 7452696241$	$(7452696241-1)/2 = 3726348120 = x_5$

Proof. From $2x + 1 = a^2$ and $3x + 1 = b^2$ comes $3a^2 - 2b^2 = 1$. If a_n, b_n is any solution of this generalized Pell equation, then

$$a_{n+1} = 5a_n + 4b_n, \quad b_{n+1} = 6a_n + 5b_n$$

is the next larger one. From these, we can obtain immediately

$$a_{n+1} + a_{n-1} = 10a_n, \quad b_{n+1} + b_{n-1} = 10b_n ,$$

which is equivalent to the algorithm.

For the n^{th} formula, we use the usual approach by linear substitution (for example, [1, p. 181]) and obtain

$$x_n = [(\sqrt{6} + 2)(5 + 2\sqrt{6})^n + (\sqrt{6} - 2)(5 - 2\sqrt{6})^n]^2/48 - 1/2 .$$

This formula has three shortcomings: (1) it uses fractions, (2) it employs roots, and (3) it has n in the exponent. The algorithm above has none of them.

Similar arguments are valid for a four-step iteration algorithm [4] to generate x in $x^2 + (x + 1)^2 = y^2$.

Sometimes, the n^{th} term formula may be simple, as for $a^2 + b^2 + (ab)^2 = c^2$, a and b consecutive positive integers [2]. Here, we have

$$(n - 1)^2 + n^2 + (n - 1)n^2 = (n^2 - n + 1)^2 ,$$

and hence we need no algorithm. But for a = 1, an algorithm would be helpful. Let us first find some clues to such an algorithm. We have by hand and by a table of squares:

$$1^2 + 0^2 + 0^2 = 1^2 = (0^2 + 1)^2$$
$$1^2 + 2^2 + 2^2 = 3^2 = (2^2 - 1)^2$$
$$1^2 + 12^2 + 12^2 = 17^2 = (4^2 + 1)^2$$
$$1^2 + 70^2 + 70^2 = 99^2 = (10^2 - 1)^2 .$$

The alternating +1 and -1 in the last column, which shows a constant pattern, suggests the possibility of an algorithm. If we can find all b, say from $b_3 = 12$ on, we will also have all c. After some trials and errors we obtain

Iteration Algorithm I

$$6 \cdot 2 - 0 = 12$$
$$6 \cdot 12 - 2 = 70$$
$$6 \cdot 70 - 12 = 408$$
$$6 \cdot 408 - 70 = 2378$$
$$6 \cdot 2378 - 408 = 13860$$
$$6 \cdot 13860 - 2378 = 80782$$

which yields easily the next four results:

$$1^2 + 408^2 + 408^2 = 577^2 = (24^2 + 1)^2$$
$$1^2 + 2378^2 + 2378^2 = 3363^2 = (58^2 - 1)^2$$
$$1^2 + 13860^2 + 13860^2 = 19601^2 = (140^2 + 1)^2$$
$$1^2 + 80782^2 + 80782^2 = 114243^2 = (338^2 - 1)^2$$

Similarly, we approach the case $a = 2$, We have by hand and by a table of squares:

$$2^2 + 1^2 + 2^2 = 3^2 = (1^2 + 2)^2$$
$$2^2 + 3^2 + 6^2 = 7^2 = (3^2 - 2)^2$$
$$2^2 + 8^2 + 16^2 = 18^2 = (4^2 + 2)^2$$
$$2^2 + 21^2 + 42^2 = 47^2 = (7^2 - 2)^2$$

The alternating +2 and −2 in the last column, which shows a constant pattern, suggest the possibility of an algorithm. If we can find all b, say from $b_3 = 8$ on, we will also have all c. After some trials and errors we obtain

Iteration Algorithm II

$$3 \cdot 3 - 1 = 8$$
$$3 \cdot 8 - 3 = 21$$
$$3 \cdot 21 - 8 = 55$$
$$3 \cdot 55 - 21 = 144$$
$$3 \cdot 144 - 55 = 377$$
$$3 \cdot 377 - 144 = 987$$

which yields easily the next four results:

$$2^2 + 55^2 + 110^2 = 123^2 = (11^2 + 2)^2$$
$$2^2 + 144^2 + 288^2 = 322^2 = (18^2 - 2)^2$$
$$2^2 + 377^2 + 754^2 = 843^2 = (29^2 + 2)^2$$
$$2^2 + 987^2 + 1974^2 = 2207^2 = (47^2 - 2)^2 .$$

Slightly differently behaves the case of $a = 3$. We have by hand and by a table of squares

$$\begin{aligned}
3^2 + 0^2 + 0^2 &= 3^2 = (0^2 + 3)^2\\
3^2 + 2^2 + 6^2 &= 7^2 = (2^2 + 3)^2\\
3^2 + 4^2 + 12^2 &= 13^2 = (4^2 - 3)^2\\
3^2 + 18^2 + 54^2 &= 57^2\\
3^2 + 80^2 + 240^2 &= 253^2 = (16^2 - 3)^2\\
3^2 + 154^2 + 462^2 &= 487^2 = (22^2 + 3)^2\\
3^2 + 684^2 + 2052^2 &= 2163^2
\end{aligned}$$

Here the doubly alternating +3 and -3 in the last column would show a constant pattern, if the exceptional values 57^2 and 2163^2 could be eliminated. This suggests obviously the possibility of two algorithms. To obtain further results, we write an Integer-FORTRAN program for the IBM 1130 which yields:

$$\begin{aligned}
3^2 + 3038^2 + 9114^2 &= 9607^2 = (98^2 + 3)^2\\
3^2 + 5848^2 + 17544^2 &= 18493^2 = (136^2 - 3)^2\\
3^2 + 25974^2 + 77922^2 &= 82137^2\\
3^2 + 115364^2 + 346092^2 &= 364813^2 = (604^2 - 3)^2\\
3^2 + 222070^2 + 666210^2 &= 702247^2 = (838^2 + 3)^2\\
3^2 + 986328^2 + 2958984^2 &= 3119043^2\\
3^2 + 4380794^2 + 13142382^2 &= 13853287^2 = (3722^2 + 3)^2
\end{aligned}$$

Now we want to find an algorithm which should generate the sequence 80, 154, 3038, 5848, 115364, 222070, 4380794, $\cdots$. Let the terms $b_1 = 0$, $b_2 = 2$, and $b_3 = 4$ be given; then $b_0 = -4$ is the left neighbor of $b_1 = 0$, since

$$3^2 + (-4)^2 + (-12)^2 = 13^2 = (4^2 - 3)^2$$

is the logical extension to the left. With this new initializing and some trials and errors, we obtain the Iteration Algorithm III on the following page. Now there remains only to find an algorithm which should generate 25974, 986328, $\cdots$. Here, we have not far to go, since such an algorithm is already contained in the former one, and we obtain Iteration Algorithm IV on the following page.

Iteration Algorithm III

$$38\cdot 2 - (-4) = 80$$
$$2\cdot 80 - 2\cdot 4 + 2 = 154$$
$$38\cdot 80 - 2 = 3038$$
$$2\cdot 3038 - 2\cdot 154 + 80 = 5848$$
$$38\cdot 3038 - 80 = 115364$$
$$2\cdot 115364 - 2\cdot 5848 + 3038 = 222070$$
$$38\cdot 115364 - 3038 = 4380794$$

Iteration Algorithm IV

$$38\cdot 684 - 18 = 25974$$
$$38\cdot 25974 - 684 = 986328$$

Finally, one could ask: Does there exist a general formula for solving $x^2 + y^2 + z^2 = w^2$? The answer is yes. Let

$$x = p^2 + q^2 - r^2, \qquad y = 2pr, \qquad z = 2qr, \qquad \text{and} \qquad w = p^2 + q^2 + r^2;$$

then $x^2 + y^2 + z^2 = w^2$ becomes $0 = 0$. But this formula has two shortcomings: (a) it uses fractions, and (b) it employs roots, since, for example, the solution $3^2 + 2^2 + 6^2 = 7^2$ requires $p = \sqrt{2}/2$, $q = 3\sqrt{2}/2$, and $r = \sqrt{2}$.

Now we shall prove how the integer solutions of certain Diophantine equations of the second degree, equivalent to Iteration Algorithms I–IV, can be found by recursive sequences. We will consider the equation

$$x^2 - (k^2 + 1)y^2 = k^2 \tag{1}$$

with $k = 1, 2$, and 3. Further, x_n and y_n will denote integer solutions of (1).

If $k = 1$, Eq. (1) becomes $x^2 - 2y^2 = 1$. By Theorem 3 of [3], the recurrence formula for this equation is given by

$$y_n = 6y_{n+1} - y_{n-1}, \qquad n > 2,$$

with $y_1 = 2$ and $y_2 = 12$.

If k = 2, Eq. (1) becomes

$$x^2 - 5y^2 = 4 . \tag{2}$$

This equation belongs to the quadratic field $Q(\theta)$, $\theta = \sqrt{5}$, which has $(1, (1+\theta)/2)$ as an integral basis, and its fundamental unit is $\epsilon_0 = (1+\theta)/2$. Since the class number of $Q(\theta)$ is 1 and the discriminant $D \equiv 5 \pmod 8$, the ideal (2) is prime [5, p. 66]. Hence, all the algebraic integers of $Q(\theta)$ of norm 4 are associates of 2. Thus, if $x_n + y_n\theta$ is an algebraic integer of norm 4, we get

$$x_n + y_n\theta = 2\epsilon_0^{2n} = 2\epsilon_1^n ,$$

where $\epsilon_1 = \epsilon_0^2 = (3+\theta)/2$.

Remark. Since we want all the algebraic integers of norm 4, we have only considered the even powers of ϵ_0. Noting that

$$\epsilon_1^{n+1} = 3\epsilon_1^n - \epsilon_1^{n-1} ,$$

we obtain

$$y_{n+1} = 3y_n - y_{n-1}, \quad n > 2 ,$$

with $y_1 = 1$ and $y_2 = 3$. It can easily be shown, by using the well-known identity

$$L_n^2 - 5F_n^2 = 4(-1)^n$$

of the Lucas and Fibonacci numbers, that $y_n = F_{2n}$ and $x_n = L_{2n}$. If k = 3, Eq. (1) becomes

$$x^2 - 10y^2 = 9 . \tag{3}$$

This equation belongs to the field $Q(\theta)$, $\theta = \sqrt{10}$, which has $(1, \theta)$ as an integral basis, $\epsilon_0 = 3 + \theta$ as its fundamental unit, and class number 2.

Since the discriminant $D \equiv 1 \pmod 3$, the ideal (3) becomes P_1P_2, where P_1 and P_2 are distinct prime ideals of norm 3. Thus there are 3 distinct ideals of norm 9. Since 3, $7 - 2\theta$, $7 + 2\theta$ are non-associated integers of norm 9, all the integers of norm 9 are associates of one of these 3 integers. It follows that

$$(4) \qquad \begin{cases} x_{3n} + y_{3n}\theta = 3\epsilon_0^{2n} = 3\epsilon_1^n , \\ x_{3n+1} + y_{3n+1}\theta = (7 - 2\theta)\epsilon_0^{2n} = (7 - 2\theta)\epsilon_1^n , \\ x_{3n+2} + y_{3n+2}\theta = (7 + 2\theta)\epsilon_0^{2n} = (7 + 2\theta)\epsilon_1^n \end{cases}$$

By applying Theorem 3 of [3], we find that ϵ_1^n satisfies the recurrence formula

$$u_{n+2} = 38u_{n+1} - u_n ,$$

where u_n is either the constant term of the coefficient of θ for ϵ_1^n. Thus the recurrence formulas for Eqs. (4) are, for $n > 2$,

$$\begin{cases} b_{3n} = 38b_{3n-3} - b_{3n-6}, & b_1 = 57, & b_6 = 684, \\ b_{3n+1} = 38b_{3n-2} - b_{3n-5}, & b_1 = 2, & b_4 = 80, \\ b_{3n+2} = 38b_{3n-1} - b_{3n-4}, & b_2 = 4, & b_5 = 154 . \end{cases}$$

REFERENCES

1. Irving Adler, "Three Diophantine Equations," Fibonacci Quarterly, 6 (1968), pp. 360-369; 7 (1969), pp. 181-193.
2. American Mathematical Monthly, 76 (1969), p. 187.
3. E. I. Emerson, "Recurrent Sequences in the Equation $DQ^2 = R^2 + N$, Fibonacci Quarterly, 7 (1969), pp. 231-242.
4. Edgar Karst, "A Four-Step Iteration Algorithm to Generate x in $x^2 + (x + 1)^2 = y^2$," Fibonacci Quarterly, 7 (1969), p. 180.
5. H. B. Mann, Introduction to the Theory of Algebraic Numbers, The Ohio State University Press, Columbus, Ohio, 1956.
6. Zentralblatt für Mathematik, 151 (1968), pp. 211-212.