ON THE DIOPHANTINE EQUATION $\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2}$

Ming Luo
Department of Mathematics, Chongqing Teachers' College
Sichuan Province, 630047, People's Republic of China
(*Submitted October 1994*)

Positive integers of the form $\frac{1}{2}m(m-1)$ are called *triangular numbers*. The Diophantine equation

$$\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2} \tag{1}$$

corresponds to the question: For which triangular numbers are their squares still triangular [1]? In 1946, Ljunggren [2] solved this problem when he proved the following.

Theorem: The Diophantine equation (1) has only the following solutions in positive integers: $(x, y) = (1, 1)$, $(2, 2)$, and $(4, 9)$.

That is, only the two triangular numbers 1 and 36 can be represented as squares of numbers of the same form. However, Ljunggren used his knowledge of the biquadratic field $Q(2^{1/4})$ and the p-adic method, so his proof is somewhat complex. In 1965, Cassels [3] gave a much simpler proof, but he also used his knowledge of the biquadratic field $Q((-2)^{1/4})$. In 1989, Cao [4] conjectured that (1) could be solved by the method of recurrent sequences. We verify his conjecture in this paper by giving the theorem and an elementary as well as simple proof by the method of recurrent sequences without using anything deeper than reciprocity.

Proof of the Theorem: Let $X = 2x-1$ and $Y = 2y-1$, then equation (1) may be reduced to $Y^2 - 2\left(\frac{X^2-1}{4}\right)^2 = 1$. Since $u + v\sqrt{2} = u_n + v_n\sqrt{2} = (1+\sqrt{2})^n$ gives the general solution of the Pellian equation $u^2 - v^2 = (-1)^n$, where $1+\sqrt{2}$ is its fundamental solution and n is an arbitrary integer (see, e.g., [1]), we get

$$X^2 = 4v_n + 1, \quad 2|n. \tag{2}$$

The following relations may be derived easily from the general solution of Pell's equation:

$$u_{n+2} = 2u_{n+1} + u_n, \qquad u_0 = 1,\ u_1 = 1; \tag{3}$$

$$v_{n+2} = 2v_{n+1} + v_n, \qquad v_0 = 0,\ v_1 = 1; \tag{4}$$

$$u_{2n} = u_n^2 + 2v_n^2, \qquad v_{2n} = 2u_nv_n; \tag{5}$$

$$v_{-n} = (-1)^{n+1}v_n; \tag{6}$$

$$v_{n+2k} \equiv (-1)^{k+1}v_n \pmod{u_k}. \tag{7}$$

If $n < 0$, then $4v_n + 1 < 0$, and (2) is impossible. Hence, it is necessary that $n \geq 0$. We shall prove that (2) cannot hold for any $n > 4$ by showing that $4v_n + 1$ is a quadratic nonresidue modulo some positive integer.

First, we consider the following three cases:

Case 1. If $n \equiv 0 \pmod 6$ and $n > 0$, then we write $n = 3^r(6k \pm 2)$, $4 \geq 1$. Let $m = 3^r$, then, by (6) and (7), we get $v_n \equiv v_{\pm 2m} \equiv \pm v_{2m} \pmod{u_{3m}}$. Since $u_{3m} = u_m(u_m^2 + 6v_m^2)$, we obtain $4v_n + 1 \equiv \pm 4v_{2m} + 1 \pmod{u_m^2 + 6v_m^2}$.

Note that $2 \nmid m$ implies $u_m^2 + 6v_m^2 \equiv 7 \pmod 8$ and $v_m \equiv 1 \pmod 4$ so, by (5), we obtain

$$\left(\frac{4v_{2m}+1}{u_m^2+6v_m^2}\right) = \left(\frac{8u_m v_m - u_m^2 + 2v_m^2}{u_m^2+6v_m^2}\right) = \left(\frac{8v_m(u_m+v_m)}{u_m^2+6v_m^2}\right)$$

$$= \left(\frac{(u_m+v_m)/2^s}{u_m^2+6v_m^2}\right) \qquad \text{(where } 2^s \| u_m + v_m\text{)}$$

$$= \left(\frac{-1}{(u_m+v_m)/2^s}\right)\left(\frac{u_m^2+6_m^2}{(u_m+v_m)/2^s}\right)$$

$$= \left(\frac{-1}{(u_m+v_m)/2^s}\right)\left(\frac{7}{(u_m+v_m)/2^s}\right) = \left(\frac{u_m+v_m}{7}\right).$$

Similarly,

$$\left(\frac{-4v_{2m}+1}{u_m^2+6v_m^2}\right) = \left(\frac{-u_m+v_m}{7}\right).$$

Equations (3) and (4) modulo 7 yield two residue sequences with the same period of 6. Since $m \equiv 3 \pmod 6$, we have $\pm u_m + v_m \equiv 5 \pmod 7$, so that

$$\left(\frac{4v_n+1}{u_m^2+6v_m^2}\right) = \left(\frac{5}{7}\right) = -1,$$

and (2) cannot hold.

Case 2. If $n \equiv 2 \pmod 4$ and $n > 2$, then we write $n = 2 + 2 \cdot 3^r \cdot m$, where $r \geq 0$, $m \equiv \pm 2 \pmod 6$. By (7), we have $4v_n + 1 \equiv -4v_2 + 1 \equiv -7 \pmod{u_m}$,

$$\left(\frac{4v_n+1}{u_m}\right) = \left(\frac{-7}{u_m}\right) = \left(\frac{u_m}{7}\right) = \left(\frac{3}{7}\right) = -1,$$

so that (2) cannot hold.

Case 3. If $n \equiv 4 \pmod{60}$ and $n > 4$, then we write $n = 4 + 2 \cdot 3 \cdot 5 \cdot k \cdot 2^r$, where $r \geq 1$, $2 \nmid k$. Let $m = 2^r$ or $3 \cdot 2^r$ or $15 \cdot 2^r$ (to be determined). By (7), we have $4v_n + 1 \equiv -4v_4 + 1 \equiv -47 \pmod{u_m}$,

$$\left(\frac{4v_n+1}{u_m}\right) = \left(\frac{-47}{u_m}\right) = \left(\frac{u_m}{47}\right).$$

The residue sequence of (3) modulo 47 has period 46. The period, with respect to r, of the residue sequence of $\{2^r\}$ modulo 46 is 11. We determine our choice of m as follows:

$$m = \begin{cases} 2^r, & \text{if } r \equiv 3, 5, 6, 7, 8, 9 \pmod{11}, \\ 3 \cdot 2^r, & \text{if } r \equiv 0, 1, 10 \pmod{11}, \\ 15 \cdot 2^r & \text{if } r \equiv 2, 4 \pmod{11}, \end{cases}$$

from which we obtain the following table.

$r \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$2^r \pmod{46}$				8		32	18	36	26	6	
$3 \cdot 2^r \pmod{46}$	26	6									36
$15 \cdot 2^r \pmod{46}$			14		10						
$u_m \pmod{47}$	35	5	33	13	26	33	15	26	35	5	26

It is easy to verify that each of the u_m in this table is a quadratic nonresidue modulo 47, from which it follows that (2) is impossible.

The three cases above tell us that, for (2) to hold, n must satisfy one of the following conditions:

$$n = 0, 2, 4;$$

or

$$n \equiv 8, 16, 20, 28, 32, 40, 44, 52, 56 \pmod{60}. \tag{8}$$

We now exclude all residues in (8) by considering some moduli of the sequence $\{4v_n + 1\}$.

First, consider modulo 5. The residue sequence of $\{4v_n + 1\}$ has period 12. If $n \equiv 8$ (mod 12), then $4v_n + 1 \equiv 3$ (mod 5), which implies that (2) is impossible. Thus, we exclude $n \equiv 8$, 20, 32, 44, 56 (mod 60) in (8).

Second, consider modulo 31. We get the residue sequence of $\{4v_n + 1\}$ having a period 30. If $n \equiv 10, 16, 22, 28 \pmod{30}$, then $4v_n + 1 \equiv 27, 17, 12, 24 \pmod{31}$, respectively. However, all of these are quadratic nonresidue modulo 31; thus, (2) cannot hold. Hence, we can exclude in (8) the other four residue classes of $n \equiv 16, 28, 40, 52 \pmod{60}$.

Finally, we look at the three values of $n = 0, 2, 4$, which give $X = 1, 3, 7$, respectively, in (2). Therefore, we see that all positive integer solutions of (1) are $(x, y) = (1, 1), (2, 2)$, and $(4, 9)$ and the proof is complete.

REFERENCES

1. L. J. Mordell. *Diophantine Equations*, pp. 268-69. London: Academic Press, 1969.
2. W. Ljunggren. "Solution complète de quelques équations du sixième degré à deux indéterminées." *Arch. Math. Naturv.* **48.7** (1946):26-29.
3. J. W. S. Cassels. "Integral Points on Certain Elliptic Curves." *Proc. Lond. Math. Soc.* (3) **14A** (1965):55-57.
4. Z. Cao. *Introduction to Diophantine Equations* (in Chinese), pp. 290-91. Harbin Industrial University Press, 1989.

AMS Classification Numbers: 11D25

❖❖❖