ON THE FORM OF SOLUTIONS OF MARTIN DAVIS' DIOPHANTINE EQUATION

Anatoly S. Izotov
Mining Institute, Novosibirsk, Russia
(Submitted September 1997-Final Revision February 1998)

1. INTRODUCTION

M. Davis proved in [1] that, if the Diophantine equation

$$9(u^2+7v^2)^2-7(r^2+7s^2)^2=2 \tag{1}$$

had no nontrivial solutions other than $u=v=1$, $r=s=0$, in nonnegative integers, then Hilbert's Tenth Problem would be unsolvable. J. Robinson proved that Hilbert's Tenth Problem would be unsolvable if (1) had only finitely many solutions.

In [3], O. Herrmann proved the existence of nontrivial solutions of (1) and D. Shanks [5] solved (1) explicitly.

D. Shanks and S. S. Wagstaff [6] found 48 more solutions of (1). They also conjectured that this equation has infinitely many solutions and gave an elaborate argument in this direction.

In this note, it is proved that solutions of (1) are members of a certain Lucas sequence and its form is described.

2. REPRESENTATION OF A_nB_n AS A MEMBER OF A RECURRENCE OF ORDER TWO

Herrmann [2] considered the Pell-like equation

$$9A_n^2-7B_n^2=2. \tag{2}$$

He proved that, if $A_0=1$, $B_0=1$, then

$$A_{n+1}=8A_n+7B_n \quad \text{and} \quad B_{n+1}=9A_n+8B_n \tag{3}$$

give all positive solutions of (2).

If A_n has the form u^2+7v^2 and B_n has the form r^2+7s^2, then every solution of (2) is a solution of (1).

By the first equation of (3), we have

$$7B_n=A_{n+1}-8A_n \quad \text{and} \quad 7B_{n+1}=A_{n+2}-8A_{n+1}, \tag{4}$$

while, by the second equation of (3), we see that $7B_{n+1}=63A_n+8\cdot 7B_n$ and, by (4), that

$$A_{n+2}-8A_{n+1}=63A_n+8(A_{n+1}-8A_n)$$

or

$$A_{n+2}=16A_{n+1}-A_n,\ A_0-1,\ A_1=15. \tag{5}$$

Analogously,

$$B_{n+2}=16B_{n+1}-B_n,\ B_0=1,\ B_1=17. \tag{6}$$

Now, consider the recurrence

$$U_{n+2}=16U_{n+1}-U_n,\ U_0=0,\ U_1=1. \tag{7}$$

By the theory of integer linear recurrences of order two, $A_n = U_{n+1} - U_n$, $B_n = U_{n+1} + U_n$, and

$$A_n B_n = U_{n+1}^2 - U_n^2 = U_{2n+1}. \tag{8}$$

Let S be the set of all odd positive numbers that have the form $x^2 + 7y^2$ for any integers x, y. The criterion for an odd $z \in S$ is:

$$\begin{aligned} &z \in S \text{ if and only if, for some prime } p,\ p^k \| z, \text{ then } p^k \in S; \\ &p^k \in S \text{ if and only if } p^k \equiv 0, 1, 2, \text{ or } 4 \pmod 7. \end{aligned} \tag{9}$$

By the criterion for integer $z \in S$, we have

$$\begin{aligned} &\text{if } z_1 \in S,\ z_2 \in S, \text{ then } z_1 z_2 \in S, \\ &\text{if } z = z_1 z_2,\ (z_1, z_2) = 1, \text{ and } z \in S, \text{ then } z_1 \in S,\ z_2 \in S. \end{aligned} \tag{10}$$

It is clear that a solution A_n, B_n of (2) is a solution of (1) if and only if $A_n \in S$, $B_n \in S$. Since $(A_n, B_n) = 1$, we see by (8) that A_n, B_n is a solution of (2) if and only if $U_{2n+1} \in S$.

Later on, we shall say that $U_{2n+1} = A_n B_n$ is a solution of (2), and accordingly of (1), if A_n, B_n is a solution of (2). The notations U_n and $U(n)$ are considered to be equivalent.

It is known that $\{U_i\}$ is periodic modulo 7 and its period is $\{1, 2, 3, 4, 5, 6, 0\}$. By (9) and (10), if $U_m \in S$ and m is odd, then

$$m \equiv 1, 7, 9, 11 \pmod{14}. \tag{11}$$

3. SOME PROPERTIES OF $U(m)$

In what follows, we shall need some properties of recurrence (7), which we give here without proofs, since they can be found in [2] and [4].

Let m_1 and m_2 be positive integers. Then

$$U(m_i) | U(m_1 m_2),\ i = 1, 2, \tag{A}$$

$$(U(m_1 m_2) / U(m_2), U(m_2)) = (m_1, U(m_2)). \tag{B}$$

If p_1 and p_2 are primes not equal to 3 or 7 and $p_1 \le p_2$, then, for $k > 0$,

$$(p_1, U(p_2^k)) = 1. \tag{C}$$

If the prime q has the form $q = 2 \cdot N + (7/q)$, where $(7/q)$ is the Legendre symbol, then

$$q | U(N). \tag{D}$$

4. "PRIME" AND "COMPOSITE" SOLUTIONS

Let U_m be a solution of (1). We say that m is a "prime" solution if m is prime and a "composite" solution if m is a composite number. By the properties of integer linear recurring sequences of order two, if m is a "composite" solution, then there exists a "prime" solution.

Theorem 1: Let m be an odd composite number, $m = p_1^{k_1} \cdots p_d^{k_d}$, $2 < p_1 < p_2 < \cdots < p_d$, $k_i > 0$. If $d = 1$, then $k_1 > 1$. Let $U(m) \in S$. Then, for all $i = 1, 2, \ldots, d$, $p_i \in S$, and for all k, $1 \le k \le k_i$, $U(p_i^k) \in S$.

Proof: We shall prove the theorem by induction on d.

(i) Let $d = 1$ and $m = p_1^{k_1}$, $k_1 > 1$. For $0 < k < k_1$, by (A) we have

$$U(p_1^{k_1}) = U(p_1^{k_1}) / U(p_1^k) \cdot U(p_1^k).$$

By (B),

$$(U(p_1^{k_1}) / U(p_1^k),\ U(p_1^k)) = (p_1^{k_1-k}, U(p_1^k)) = 1 \quad \text{for } p_1 \neq 3 \text{ or } 7.$$

Since $U(m) \in S$, we have $U(p_1^k) \in S$ for $k = 1, 2, \ldots, k_1 - 1$. So, for $k = 1$, $U(p_1) \in S$ and, by (11), $p_1 \in S$.

If $p_1 = 3$ or 7 and $U(p_1^{k_1}) \in S$, then

$$U(p_1^{k_1}) = p_1 U(p_1^{k_1}) / U(p_1) \cdot U(p_1) / p_1 \quad \text{and} \quad (p_1 U(p_1^{k_1}) / U(p_1),\ U(p_1) / p_1) = 1.$$

Therefore, $U(p_1) / p_1 \in S$, which is impossible since

$$U(3) / 3 = 5 \cdot 17 \notin S \quad \text{and} \quad U(7) / 7 = 13 \cdot 293 \cdot 617 \notin S.$$

(ii) Let $d = 2$, $m = p_1^{k_1} p_2^{k_2}$, $p_1 < p_2$, and $U(m) \in S$. Then, $U(m) = U(m) / U(p_2^{k_2}) \cdot U(p_2^{k_2})$. Since $(U(m) / U(p_2^{k_2}) \cdot U(p_2^{k_2})) = (p_1^{k_1}, U(p_2^{k_2})) = 1$ by (C), we have$U(p_2^{k_2}) \in S$ and, by (i), $p_2 \in S$, $U(p_2) \in S$.

Furthermore, $U(m) = U(m) / U(p_1^{k_1}) \cdot U(p_1^{k_1})$. Let

$$(U(m) / U(p_1^{k_1}), U(p_1^{k_1})) = (p_2^{k_2} \cdot U(p_1^{k_1})) = p_2^c, \text{ for } 0 < c \leq k_2.$$

Then, $U(m) = p_2^c \cdot U(m) / U(p_1^{k_1}) \cdot U(p_1^{k_1}) / p_2^c$ and $M = U(p_1^{k_1}) / p_2^c \in S$. Since $p_2 \in S$, $p_2^c \in S$, and $M p_2^c = U(p_1^{k_1}) \in S$. By (i), we have $U(p_1) \in S$, $p_1 \in S$.

(iii) Assume that the statements of Theorem 1 are true for $1 < t < d$. Then, for $t = d$, let $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_d^{k_d}$, $p_1 < p_2 < \cdots < p_d$, and $U(m) \in S$. Also, let $m = m_1 p_d^{k_d}$. By (ii), $p_d > 7$. Furthermore, $U(m) = U(m) / U(p_d^{k_d}) \cdot U(p_d^{k_d})$.

Since $(U(m) / U(p_d^{k_d}), U(p_d^{k_d})) = (m_1, U(p_d^{k_d})) = 1$ by (C), we have $U(p_d^{k_d}) \in S$ and, by (i), $U(p_d) \in S$, $p_d \in S$.

Consider $U(m) = U(m) / U(m_1) \cdot U(m_1)$. Let $D = (U(m) / U(m_1), U(m_1)) = (p_d^{k_d}, U(m_1)) = p_d^c$, where $0 \leq c \leq k_d$. Then, $U(m) = D \cdot U(m) / U(m_1) \cdot U(m_1) / D$ and $M = U(m_1) / D \in S$. Since $D \in S$, we have $U(m_1) = M \cdot D \in S$ and, by the induction statements, for all i, $0 < i < d$, $p_i \in S$, $U(p_i^k) \in S$, $0 < k < k_i$, and the theorem is proved.

In [6], Daniel Shanks and Samuel S. Wagstaff conjectured that equation (1) has infinitely many solutions. Theorem 2 gives some information on the form of these solutions.

Theorem 2: If there are infinitely many solutions of (1), but only finitely many "prime" solutions, then there is at least one prime $q \in S$ such that $U(q^k) \in S$ for all $k > 0$.

Inversely, if there are infinitely many solutions of (1) and, for each prime $p \in S$, there exists $k = k(p)$ such that $U(p^k) \notin S$, then there are infinitely many "prime" solutions.

Proof: Let $\{m_i\}$, $i = 1, 2, \ldots$ be the set of solutions of (1). If $p_1, p_2, \ldots, p_d$ is the finite set of "prime" solutions of (1), then, by Theorem 1, $m_i = p_1^{k_{1i}} p_2^{k_{2i}} \cdots p_d^{k_{di}}$. Since $m_{i \to \infty} \to \infty$, there exists at least one p_j, $0 < j \leq d$ such that $k_{ji} \to \infty$ as $i \to \infty$. By Theorem 1, $U(p_j^k) \in S$ for all $k > 1$.

Inversely, if for each prime $p \in S$ there exists $k = k(q)$ and $U(p^k) \notin S$, then, by Theorem 1, $U(p^d) \notin S$ for $d \geq k(p)$. If there are finitely many "prime" solutions, then, by Theorem 1, there exist finitely many "composite" solutions only.

It is more probable that there exist infinitely many "prime" solutions. Indeed, if for each prime $p \in S$ there exists at least one prime q of the form $q = 2p^n + (7/q)$, where $(7/q)$ is the Legendre symbol, then $(q/7) = -1$ and so $q \notin S$. By (D), $q | U(p^n)$ and $(p^n) \notin S$.

5. ON "COMPOSITE" SOLUTIONS

In [6], the solution $p_1 = 53$ was given and two new solutions of equation (1) were found: $p_2 = 67$ and $p_3 = 71$. By Theorem 1, the corresponding "composite" solutions have the form $m = p_1^a p_2^b p_3^c$, $a, b, c \geq 0$. To test whether there are "composite" solutions, it is sufficient to consider $m_1 = p_1^2, m_2 = p_1 p_2, m_3 = p_1 p_3, m_4 = p_2^2, m_5 = p_2 p_3$, and $m_6 = p_3^2$.

A computer examination produced the following:

For $m_1 = 53^2 = 2809$, $U(m_1)$ has no prime divisors up to $1 \cdot 10^9$.

For $m_2 = 53 \cdot 67 = 3551$, $7103 \| U(m_2)$, and $7103 \notin S$, so $U(m_2) \notin S$.

For $m_3 = 53 \cdot 71 = 3763$, $1979339 \| U(m_3)$, and $1979339 \notin S$, so $U(m_3) \notin S$.

For $m_4 = 67^2 = 4489$, $673349 \| U(m_4)$, and $673349 \notin S$, so $U(m_4) \notin S$.

For $m_5 = 67 \cdot 71 = 4757$, $332989 \| U(m_5)$, and $332989 \notin S$, so $U(m_5) \notin S$.

For $m_6 = 71^2 = 5041$, $46427611 \| U(m_6)$, and $46427611 \notin S$, so $U(m_6) \notin S$.

Note that:

For $m_7 = 53^3 = 148877$, $893261 \| U(m_7)$, and $893261 \notin S$, so $U(m_7) \notin S$.

Perhaps the only "composite" solution of (1) of the form $m = p_1^a p_2^b p_3^c$ is $m_1 = 53^2 = 2809$, and it is the least "composite" solution.

REFERENCES

1. Martin Davis. "One Equation To Rule Them All." *Trans. New York Acad. Sci.* (II) **30** (1968):766-73.
2. H. J. A. Duparc. "Periodicity Properties of Recurring Sequences, II." *Proc. Koninkl. Nederl. Acad. Wetensch*, A57, **4** (1954):473-85.
3. Oskar Herrmann. "A Non-Trivial Solution of the Diophantine Equation $9(x^2 + y^2)^2 - 7(u^2 + v^2)^2 = 2$." In *Computers in Number Theory*, pp. 207-12. London: Academic Press, 1971.
4. Dov Jarden. *Recurring Sequences*. Jerusalem: Riveon Lematematika, 1966.
5. Daniel Shanks. "Five Number-Theoretic Algorithms." In *Proc. of the Second Manitoba Conference on Numerical Mathematics*, pp. 51-70. Winnipeg: Univ. of Manitoba, 1972.
6. Daniel Shanks & Samuel S. Wagstaff. "48 More Solutions of Martin Davis's Quaternary Quartic Equation." *Math. Comp.* **64** (1995):1717-31.

AMS Classification Numbers: 11B25, 11B37

❖❖❖