LUCAS AND FIBONACCI NUMBERS AND SOME DIOPHANTINE EQUATIONS

by J. H. E. COHN

(Received 11 February, 1964)

1. Introduction. The Lucas numbers v_n and the Fibonacci numbers u_n are defined by $v_1 = 1$, $v_2 = 3$, $v_{n+2} = v_{n+1} + v_n$ and $u_1 = u_2 = 1$, $u_{n+2} = u_{n+1} + u_n$ for all integers n. The elementary properties of these numbers are easily established; see for example [2]. However, despite the ease with which many such properties are proved, there are a number of more difficult questions connected with these numbers, of which some are as yet unanswered. Among these there is the well-known conjecture that u_n is a perfect square only if $n = 0, \pm 1, 2$ or 12. This conjecture was proved correct in [1]. The object of this paper is to prove similar results for v_n, $\frac{1}{2}u_n$ and $\frac{1}{2}v_n$, and incidentally to simplify considerably the proof for u_n. Secondly, we shall use these results to solve certain Diophantine equations.

2. Preliminaries. We shall require the following results which are easily proved from the definitions:

$$2u_{m+n} = u_m v_n + u_n v_m, \tag{1}$$

$$2v_{m+n} = 5u_m u_n + v_m v_n, \tag{2}$$

$$v_{2m} = v_m^2 + (-1)^{m-1}2, \tag{3}$$

$$(u_{3m}, v_{3m}) = 2, \tag{4}$$

$$(u_n, v_n) = 1 \text{ if } 3 \mid n, \tag{5}$$

$$2 \mid v_m \quad \text{if and only if} \quad 3 \nmid m, \tag{6}$$

$$3 \mid v_m \quad \text{if and only if} \quad m \equiv 2 \pmod 4, \tag{7}$$

$$u_{-n} = (-1)^{n-1} u_n, \tag{8}$$

$$v_{-n} = (-1)^n v_n, \tag{9}$$

$$v_k \equiv 3 \pmod 4 \quad \text{if} \quad 2 \mid k,\ 3 \nmid k, \tag{10}$$

We shall throughout this paper reserve the symbol k to denote an integer, not necessarily positive, which is even but not divisible by 3. We shall now prove the following two results:

$$v_{m+2k} \equiv -v_m \pmod{v_k}, \tag{11}$$

$$u_{m+2k} \equiv -u_m \pmod{v_k}, \tag{12}$$

For, by (1), (2) and (3),

$$\begin{aligned} 2v_{m+2k} &= 5u_m u_{2k} + v_m v_{2k} \\ &= 5u_m u_k v_k + v_m (v_k^2 - 2) \\ &\equiv -2v_m \pmod{v_k}, \end{aligned}$$

https://doi.org/10.1017/S2040618500035115 Published online by Cambridge University Press

and so (11) follows, by (10). Similarly,

$$\begin{aligned} 2u_{m+2k} &= u_m v_{2k} + u_{2k} v_m \\ &= u_m(v_k^2 - 2) + u_k v_k v_m \\ &\equiv -2u_m \pmod{v_k}, \end{aligned}$$

and (12) follows.

3. The main theorems.

THEOREM 1. *If* $v_n = x^2$, *then* $n = 1$ *or* 3; *i.e.* $x = \pm 1$ *or* ± 2.

Proof. (i) If n is even, then, by (3),

$$v_n = y^2 \pm 2 \neq x^2.$$

(ii) If $n \equiv 1 \pmod 4$, then $v_1 = 1$, whereas if $n \neq 1$ we can write $n = 1 + 2 \,.\, 3^r \,.\, k$ where $r \geqq 0$ and k has the required properties of being even and not divisible by 3. Then repeated application of (11) gives

$$v_n \equiv (-1)^{3^r} v_1 \equiv -1 \pmod{v_k}.$$

Hence, by (10), $(v_n \mid v_k) = -1$ and so $v_n \neq x^2$.

(iii) If $n \equiv 3 \pmod 4$, then $v_3 = 2^2$, whereas if $n \neq 3$, $n = 3 + 2 \,.\, 3^r \,.\, k$ and as before

$$v_n \equiv -v_3 \equiv -4 \pmod{v_k}.$$

Now, by (10), v_k is odd and so

$$(v_n \mid v_k) = (4 \mid v_k)(-1 \mid v_k) = -1$$

and $v_n \neq x^2$. This concludes the proof.

THEOREM 2. *If* $v_n = 2x^2$, *then* $n = 0$ *or* ± 6; *i.e.* $x = \pm 1$ *or* ± 3.

Proof. (i) If n is odd and v_n is even, then by (6), $3 \mid n$ and so $n \equiv \pm 3 \pmod{12}$. Now by (2)

$$\begin{aligned} 2v_{m+12} &= 5u_m u_{12} + v_m v_{12} = 720 u_m + 322 v_m \\ &\equiv 2v_m \pmod{16}. \end{aligned}$$

Hence $$2v_n \equiv 2v_{\pm 3} \equiv 8 \pmod{16}$$

and so $v_n \neq 2x^2$.

(ii) If $n \equiv 0 \pmod 4$, then $v_0 = 2$, whereas if $n \neq 0$, $n = 2 \,.\, 3^r \,.\, k$ and so by (11),

$$2v_n \equiv -2v_0 \equiv -4 \pmod{v_k},$$

so that $2v_n \neq y^2$, i.e. $v_n \neq 2x^2$.

(iii) If $n \equiv 6 \pmod 8$, then $v_6 = 2 \,.\, 3^2$, whereas if $n \neq 6$, $n = 6 + 2 \,.\, 3^r \,.\, k$, where $4 \mid k$ and $3 \nmid k$. Hence

$$2v_n \equiv -2v_6 \equiv -36 \pmod{v_k}.$$

https://doi.org/10.1017/S2040618500035115 Published online by Cambridge University Press

Now by (10), v_k is odd, and since $4 \mid k$, $3 \nmid v_k$ by (7). Hence 36 has no factor in common with v_k, and so as before $v_n \neq 2x^2$.

(iv) If $n \equiv 2 \pmod 8$, then by (9) $v_{-n} = v_n$, where now $-n \equiv 6 \pmod 8$. Hence by (iii) $v_n = 2x^2$ if and only if $-n = 6$, i.e. $n = -6$.

This concludes the proof.

THEOREM 3. *If* $u_n = x^2$, *then* $n = 0, \pm 1, 2$ *or* 12; *i.e.* $x = 0, \pm 1$ *or* ± 12.

Proof. (i) If $n \equiv 1 \pmod 4$, then $u_1 = 1$, whereas if $n \neq 1$, $n = 1+2.3^r.k$ and so

$$u_n \equiv -u_1 \equiv -1 \pmod{v_k},$$

so that $u_n \neq x^2$.

(ii) If $n \equiv 3 \pmod 4$, then $u_{-n} = u_n$ by (8), and so $u_n = x^2$ if and only if $-n = 1$, i.e. $n = -1$.

(iii) If n is even, then $u_n = x^2$ gives, by (1),

$$x^2 = u_n = u_{n/2} v_{n/2}$$

and so (4) and (5) give two possibilities:

(*a*) $3 \mid n$, $u_{n/2} = 2y^2$; $v_{n/2} = 2z^2$. By Theorem 2, the second of these is satisfied only by $\frac{1}{2}n = 0, 6$ or -6. However the last of these must be rejected since it does not satisfy $u_{n/2} = 2y^2$.

(*b*) $3 \nmid n$, $u_{n/2} = y^2$; $v_{n/2} = z^2$. By Theorem 1, the second of these is satisfied only for $\frac{1}{2}n = 1$ (and $\frac{1}{2}n = 3$ which must be rejected since $3 \nmid n$).

Hence we have in all the five values, $n = 0, \pm 1, 2$ or 12.

THEOREM 4. *If* $u_n = 2x^2$, *then* $n = 0, \pm 3$ *or* 6; *i.e.* $x = 0, \pm 1$ *or* ± 2.

Proof. (i) If $n \equiv 3 \pmod 4$, then $u_3 = 2$, whereas if $n \neq 3$, $n = 3+2.3^r.k$ and so

$$2u_n \equiv -2u_3 \equiv -4 \pmod{v_k},$$

so that $u_n \neq 2x^2$.

(ii) If $n \equiv 1 \pmod 4$, then $u_n = u_{-n}$ by (8) and so $u_n = 2x^2$ if and only if $-n = 3$, i.e. $n = -3$.

(iii) If n is even, then

$$2x^2 = u_n = u_{n/2} v_{n/2},$$

by (1), and so by (4) and (5) we have the following two possibilities:

(*a*) $u_{n/2} = y^2$; $v_{n/2} = 2z^2$. Theorems 2 and 3 show that the only value of n which satisfies both of these is $n = 0$.

(*b*) $u_{n/2} = 2y^2$; $v_{n/2} = z^2$. The latter is satisfied only for $\frac{1}{2}n = 1$ or 3, by Theorem 1, and since $\frac{1}{2}n = 1$ does not satisfy the former, we get only $n = 6$.

This concludes the proof.

4. Eight Diophantine equations. We shall now solve eight Diophantine equations; since in all of them only even powers of x occur, we shall only list the non-negative solutions. As a first step we shall introduce the numbers $a = \frac{1}{2}(1+\sqrt{5})$ and $b = \frac{1}{2}(1-\sqrt{5})$. It is then easily shown that $u_n = 5^{-\frac{1}{2}}(a^n - b^n)$ and $v_n = a^n + b^n$. We now prove the following results.

1. *The equation $y^2 = 5x^4+1$ has only the solutions $x = 0, 2$.*

(Professor L. J. Mordell has just informed me that he has proved this; see [3].)

For $y^2 - 5x^4 = 1$ and so y and x^2 are a set of solutions of the Pell equation $p^2 - 5q^2 = 1$. Thus, for some value of the integer n we have

$$y + x^2\sqrt{5} = (9+4\sqrt{5})^n = \left\{\frac{1+\sqrt{5}}{2}\right\}^{6n};$$

i.e.

$$y + x^2\sqrt{5} = a^{6n}, \quad y - x^2\sqrt{5} = b^{6n}.$$

Thus $2x^2 = u_{6n}$ and so $x = 0$ or 2, by Theorem 4.

2. *The equation $5y^2 = x^4 - 1$ has only the solutions $x = 1, 3$.*

For $x^4 - 5y^2 = 1$ and so, as before, $x^2 + y\sqrt{5} = a^{6n}$ and $x^2 - y\sqrt{5} = b^{6n}$. Thus $2x^2 = v_{6n}$ and so $x = 1$ or 3, by Theorem 2.

3. *The equation $y^2 = 20x^4+1$ has only the solutions $x = 0, 6$.*

For $y^2 - 5(2x^2)^2 = 1$ and so $y + 2x^2\sqrt{5} = a^{6n}$ and $y - 2x^2\sqrt{5} = b^{6n}$. Hence $4x^2 = u_{6n}$, so that $x = 0$ or 6, by Theorem 3.

4. *The equation $y^2 = 5x^4 - 1$ has only the solution $x = 1$.*

For $y^2 - 5x^4 = -1$ and so, for some integer n,

$$y + x^2\sqrt{5} = (2+\sqrt{5})^{2n-1} = \left\{\frac{1+\sqrt{5}}{2}\right\}^{6n-3} = a^{6n-3},$$

and $y - x^2\sqrt{5} = b^{6-3}$. Hence $2x^2 = u_{6n-3}$ and so $x = 1$, by Theorem 4.

5. *The equation $5y^2 = 4x^4+1$ has only the solution $x = 1$.*

For $(2x^2)^2 - 5y^2 = -1$; thus $2x^2 + y\sqrt{5} = a^{6n-3}$ and $2x^2 - y\sqrt{5} = b^{6n-3}$. Hence $4x^2 = v^{6n-3}$ and so $x = 1$, by Theorem 1.

6. *The equation $y^2 = 5x^4+4$ has only the solutions $x = 0, 1, 12$.*

For $y^2 - 5x^4 = 4$. Thus, for some value of the integer n,

$$y + x^2\sqrt{5} = 2\left\{\frac{3+\sqrt{5}}{2}\right\}^n = 2a^{2n},$$

$$y - x^2\sqrt{5} = 2b^{2n}.$$

Hence $x^2 = u_{2n}$ and so $x = 0, 1$ or 12, by Theorem 3.

7. *The equation* $y^2 = 5x^4 - 4$ *has only the solution* $x = 1$.

For $y^2 - 5x^4 = -4$, and so for some value of the integer n

$$y + x^2\sqrt{5} = 2\left\{\frac{1+\sqrt{5}}{2}\right\}^{2n-1} = 2a^{2n-1},$$

$$y - x^2\sqrt{5} = 2b^{2n-1}.$$

Hence $x^2 = u_{2n-1}$ and so $x = 1$, by Theorem 3.

8. *The equation* $5y^2 = x^4 + 4$ *has only the solutions* $x = 1, 2$.

For $x^4 - 5y^2 = -4$; thus $x^2 + y\sqrt{5} = 2a^{2n-1}$ and $x^2 - y\sqrt{5} = 2b^{2n-1}$. Hence $x^2 = v_{2n-1}$ and so $x = 1, 2$, by Theorem 1.

REFERENCES

1. J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.*, **39** (1964), 537–540.
2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford, 1954), §10.14.
3. L. J. Mordell, The Diophantine equation $y^2 = Dx^4 + 1$, *J. London Math. Soc.* **39** (1964), 161–164.

Bedford College
London, N.W.1

https://doi.org/10.1017/S2040618500035115 Published online by Cambridge University Press