PACIFIC JOURNAL OF MATHEMATICS
Vol. 41, No. 3, 1972

SQUARES IN SOME RECURRENT SEQUENCES

J. H. E. COHN

Elementary methods are used to locate the perfect squares in certain sequences of integers defined by three term recurrence relations.

We consider for $n \geqq 0$ the polynomials $P_n(x)$, $Q_n(x)$, $p_n(x)$ and $q_n(x)$ defined by

$$P_0(x) = p_0(x) = 0;\ P_1(x) = p_1(x) = 1 \tag{1}$$

$$Q_0(x) = q_0(x) = 2;\ Q_1(x) = q_1(x) = x \tag{2}$$

$$P_{n+2}(x) = xP_{n+1}(x) + P_n(x) \tag{3}$$

$$Q_{n+2}(x) = xQ_{n+1}(x) + Q_n(x) \tag{4}$$

$$p_{n+2}(x) = xp_{n+1}(x) - p_n(x) \tag{5}$$

$$q_{n+2}(x) = xq_{n+1}(x) - q_n(x)\ . \tag{6}$$

These polynomials arose in a natural way in the course of previous work [2, 3] and using the result of [1] the complete solutions of the Diophantine equations $y^2 = P_n(x)$, $2y^2 = P_n(x)$ and the six similar ones obtained by substituting $Q_n(x)$, $p_n(x)$ and $q_n(x)$ for $P_n(x)$ in positive integers x, y and n, with x restricted to *odd* values, have been found. The method, although fairly long, was elementary.

The same problems for even values of x seem to be far harder, although in certain cases they may be trivial. For $x = 2$, the only significant problem is $y^2 = P_n(2)$. Ljunggren [5] has shown that $n = 0, 1, 7$ yield the only solutions in this case, but the method is non-elementary and involves much computation. It is unlikely that method could be applied to provide a complete solution in n and x. The main object of the present note is to consider an infinite set of even values of x for which an elementary method is available for the determination of n. Use is then made of these results to prove some theorems on Diophantine equations of the form $X^2 = DY^4 \pm 1$, $X^2 = DY^4 \pm 4$.

Using (1)–(6) we find easily that

$$P_n(x) = \frac{\left(\frac{x + (x^2+4)^{1/2}}{2}\right)^n - \left(\frac{x - (x^2+4)^{1/2}}{2}\right)^n}{(x^2+4)^{1/2}} \tag{7}$$

$$Q_n(x) = \left(\frac{x + (x^2+4)^{1/2}}{2}\right)^n + \left(\frac{x - (x^2+4)^{1/2}}{2}\right)^n \tag{8}$$

$$p_n(x) = \frac{\left(\frac{x + (x^2 - 4)^{1/2}}{2}\right)^n - \left(\frac{x - (x^2 - 4)^{1/2}}{2}\right)^n}{(x^2 - 4)^{1/2}} \tag{9}$$

$$q_n(x) = \left(\frac{x + (x^2 - 4)^{1/2}}{2}\right)^n + \left(\frac{x - (x^2 - 4)^{1/2}}{2}\right)^n . \tag{10}$$

For convenience we may use (3) and (5) to extend the definitions of $P_n(x)$ and $p_n(x)$ to negative values of n, yielding

$$P_{-n}(x) = (-1)^{n-1}P_n(x) \tag{11}$$

$$p_{-n}(x) = -p_n(x) . \tag{12}$$

We also obtain

$$Q_n^2(x) - (x^2 + 4)P_n^2(x) = (-1)^n 4 \tag{13}$$

$$q_n^2(x) - (x^2 - 4)p_n^2(x) = 4 \tag{14}$$

whence

$$(Q_n(x), P_n(x)) = 1 \text{ or } 2 \tag{15}$$

$$(q_n(x), p_n(x)) = 1 \text{ or } 2 . \tag{16}$$

Also using (7)-(10) with (13) and (14) we obtain

$$\text{if } m \text{ is odd,} \quad P_n(Q_m(a)) = \frac{P_{mn}(a)}{P_m(a)} , \quad Q_n(Q_m(a)) = Q_{mn}(a) \tag{17}$$

$$\text{if } m \text{ is even,} \quad p_n(Q_m(a)) = \frac{P_{mn}(a)}{P_m(a)} , \quad q_n(Q_m(a)) = Q_{mn}(a) \tag{18}$$

$$p_n(q_m(a)) = \frac{p_{mn}(a)}{p_m(a)} , \quad q_n(q_m(a)) = q_{mn}(a) . \tag{19}$$

Now suppose that $m \equiv 3 \pmod 6$ and that $x = Q_m(a)$ with a odd. Then from (17) we see that $Q_n(x) = Q_{mn}(a)$ and so using [2; Theorem 7] we find that $y^2 = Q_n(x)$ is possible only for $mn = 3$, with $a = 1$ or 3. This the only solutions are provided by $n = 1$, with $x = 4$ or 36. Similarly $2y^2 = Q_n(x)$ gives $mn = 0$, or $mn = 6$ with $a = 1$ or 5 (in view of [1]) or $m = 3$, $n = 2$, $x = 4$ or 140. Thus we have proved

THEOREM 1. *If $x = Q_m(a)$ with a odd, $m \equiv 3 \pmod 6$, then $y^2 = Q_n(x)$ is possible only for $n = 1$ with $x = 4$ or 36, and $2y^2 = Q_n(x)$ is possible only for $n = 0$, and for $n = 2$ with $x = 4$ or 140.*

We next consider $P_n(x)$ under the same conditions. We have $P_1(x) = 1$, and if $n \equiv 1 \pmod 4$, $n \neq 1$, we write $n = 1 + 2hk$, where

$k = 2^r$, $r \geqq 1$ and h is odd. Then using [2; (22)] we obtain by (17)

$$\begin{aligned} P_m(a)P_n(x) &= P_{mn}(a) \\ &\equiv (-1)^{mh}P_m(a) \pmod{Q_k(a)} \\ &\equiv -P_m(a) \pmod{Q_k(a)}, \end{aligned}$$

since mh is odd. Now it is easily verified that $P_m(a)$ and $Q_k(a)$ have no factor in common and so we obtain

$$P_n(x) \equiv -1 \pmod{Q_k(a)}$$

from which it follows that $P_n(x) \neq y^2$, since $Q_k(a) \equiv 3 \pmod 4$ in virture of [2; (16)]. Since, by (11), for n odd $P_n(x) = P_{-n}(x)$ it follows that $P_n(x) = y^2$ is possible with n odd, $n > 0$ only for $n = 1$.

Now for n even we have using (7) and (8) that

$$P_n(x) = P_{(1/2)n}(x)Q_{(1/2)n}(x)$$

and so in view of (15) $y^2 = P_n(x)$ implies

either $Q_{(1/2)n}(x) = y_1^2$; $P_{(1/2)n}(x) = y_2^2$; the former implies $1/2n = 1$ with $x = 4$ or 36, both of which satisfy the latter,
or $Q_{(1/2)n}(x) = 2y_1^2$; $P_{(1/2)n}(x) = 2y_2^2$; the former implies $1/2n = 0$ which satisfies the latter, or $1/2n = 2$ with $x = 4$ or 140, but neither of these satisfies the later.

Finally, considering $2y^2 = P_n(x)$ we see easily that since x is even, n must also be even, and we obtain as before $Q_{(1/2)n}(x) = y_1^2$ or $2y_1^2$, yielding $n = 0$ or $n = 4$, $x = 4$. Thus we have

THEOREM 2. *If $x = Q_m(a)$ with a odd, $m \equiv 3 \pmod 6$, then $y^2 = P_n(x)$ possible only for $n = 0$ and $n = 1$ and for $n = 2$ with $x = 4$ or 36; $2y^2 = P_n(x)$ is possible only for $n = 0$ and for $n = 4$ with $x = 4$.*

An exactly parallel treatment for $x = q_m(a)$ with $3 \mid m$ leads to the following results, whose proofs are omitted.

THEOREM 3. *If $x = q_m(a)$ with a odd, $3 \mid m$, then $y^2 = q_n(x)$ is impossible, and $2y^2 = q_n(x)$ is possible only for $n = 0$, and for $n = 1$ with $x = 18$ or $19{,}602$.*

THEOREM 4. *If $x = q_m(a)$ with a odd, $3 \mid m$, then $y^2 = p_n(x)$ is possible only for $n = 0$ and 1, and $2y^2 = p_n(x)$ is possible only for $n = 0$, and for $n = 2$ with $x = 18$ or $19{,}602$.*

We now prove

THEOREM 5. *The equation $y^2 = P_m(a)P_n(a)$ where a is odd and*

$m \geqq n > 0$ has only the trivial solution $m = n$, except for $a = A^2$, $m = 2$, $n = 1$; $a = 1$, $m = 12$, $n = 1$; $a = 1$, $m = 12$, $n = 2$; $a = 1$, $m = 6$, $n = 3$; $a = 3$, $m = 6$, $n = 3$.

Proof. Let $r = (m, n)$. Then as is well known

$$(P_m(a), P_n(a)) = P_r(a)$$

and so if $m = Mr$, $n = Nr$ we must have

$$y_1^2 = \frac{P_{Mr}(a)}{P_r(a)}\,; \quad y_2^2 = \frac{P_{Nr}(a)}{P_r(a)}\,.$$

We consider four cases:

(a). $2 \nmid r$, $3 \nmid r$; then using (17) we have $y_1^2 = P_M(Q_r(a))$. Since $Q_r(a)$ is odd, we have using [2; Theorem 5] that $M = 1$ or 2 or 12. Now $M = 1$ always satisfies this; $M = 2$ implies $y_1^2 = Q_r(a)$ and so $r = 1$, $a = y_1^2$; $M = 12$ implies $1 = Q_r(a)$ or $r = a = 1$.

(b). $2 | r$, $3 \nmid r$; then using (18) $y_1^2 = p_M(Q_r(a))$. Since $Q_r(a)$ is odd, we have using [3; Theorem 5] that $M = 1$ or 2 or 6. $M = 1$ always satisfies this; $M = 2$ impiles $y_1^2 = Q_r(a)$ which is impossible for r even; $M = 6$ implies $3 = Q_r(a)$ and so $r = 2$, $a = 1$.

(c). $2 \nmid r$, $3 | r$; then $y_1^2 = P_M(Q_r(a))$ and so Theorem 2 is applicable yielding $M = 1$ and $M = 2$ with $r = 3$ and $a = 1$ or 3.

(d). $6 | r$; then $y_1^2 = p_M(Q_r(a)) = p_M(x)$ where $x = Q_r(a) = q_{(1/2)r}(Q_2(a))$ using (18). Now $Q_2(a)$ is odd, and so using Theorem 4 we obtain only $M = 1$.

Combining the four cases we find that $M = 1$, except if

$$\begin{gathered} r = 1,\ a = y_1^2,\ M = 2 \\ r = 1,\ a = 1,\ M = 12 \\ r = 3,\ a = 1,\ M = 2 \\ r = 3,\ a = 1,\ M = 2 \\ r = 2,\ a = 1,\ M = 6\ . \end{gathered}$$

Similar results hold for N, and so we obtain $M = N = 1$, or $m = n$, except for

$$\begin{aligned} &r = 1,\ a = y_1^2,\ M = 2,\ N = 1 && \text{i.e. } m = 2,\ n = 1 \\ &r = 1,\ a = 1,\ M = 12,\ N = 1 && \text{i.e. } m = 12,\ n = 1 \\ &r = 3,\ a = 1,\ M = 2,\ N = 1 && \text{i.e. } m = 6,\ n = 3 \end{aligned}$$

$$r = 3,\ a = 3,\ M = 2,\ N = 1 \quad \text{i.e. } m = 6,\ n = 3$$
$$r = 2,\ a = 1,\ M = 6,\ N = 1 \quad \text{i.e. } m = 12,\ n = 2\ ,$$

and this is the required result.

THEOREM 6. *The equation* $2y^2 = P_m(a)P_n(a)$, *where* a *is odd and* $m > n > 0$ *has no solutions, the following cases only excepted,*

$a = 1$, *with* $m, n = 3, 2; 3, 1; 6, 1; 6, 2; 12, 3$ *or* $12, 6$

$a = 5$, *with* $m, n = 12, 6$

$a \neq 1$, *with* $a^2 = 2A^2 - 1$ *and* $m, n = 3, 1$.

Proof. As in the proof of the previous theorem let $r = (m, n)$, $m = Mr$, $n = Nr$ and we find that

$$y_1^2 = \frac{P_{Mr}(a)}{P_r(a)};\quad 2y_2^2 = \frac{P_{Nr}(a)}{P_r(a)}\ ,$$

or vice-versa. The former yields (since $M \neq 0$) $M = 1$, except if $a = 1$ when also $r = 2$, $M = 6$ or $r = 1$ and $M = 2$ or 12, and if $a = 3$ when also $r = 3$, $M = 2$ and if $a = A^2$ with $r = 1$, $M = 2$.

Consider now the latter with $N \neq 0$. As before we distinguish four cases.

(a). $2 \nmid r$, $3 \nmid r$; then $2y_2^2 = P_N(Q_r(a))$. Since $Q_r(a)$ is odd, we may use [2; Theorem 6] and we see that the only possibilities are $N = 6$ with $Q_r(a) = 1$, i.e. $r = a = 1$, and perhaps $N = 3$. But $N = 3$ would require $2y_2^2 = (Q_r(a))^2 + 1$, and we shall show that this is impossible except for $r = 1$.

Since r is odd, it follows from [2; (11)] that we require $Q_{2r}(a) = 2y_2^2 + 1$. If we allow the possibility of negative r, we can assume that $r \equiv 1 \pmod 4$, since we can show just as in (11) that $Q_{-n}(x) = (-1)^n Q_n(x)$. Then if $r \neq 1$, let $r = 1 + hk$, where h is odd and $k = 2^R$, with $R \geqq 2$. Thus

$$\begin{aligned} 2y_2^2 + 1 &= Q_{2r}(a) \\ &= Q_{2+2hk}(a) \\ &\equiv -Q_2(a) \qquad (\text{mod } Q_k(a)) \text{ using } [2;\ (23)] \\ &\equiv -(a^2 + 2) \qquad (\text{mod } Q_k(a))\ . \end{aligned}$$

From [2; (16), (17)] we see that $Q_k(a) \equiv 7 \pmod 8$ since $R \geqq 2$, and so we should have to have

$$\begin{aligned} 1 &= (y_2^2 \,|\, Q_k(a)) \\ &= (-2 \,|\, Q_k(a))\Big(\frac{a^2 + 3}{4}\Big|\, Q_k(a)\Big) \end{aligned}$$

$$= -1 \quad \text{in view of [2; (27), (28)] since } Q_k(a) \equiv 7 \pmod 8 ,$$

and this contradiction shows that we can have only $r = 1$.

For this to occur we must have $r = 1$, $N = 3$, $a^2 = 2y_2^2 - 1$.

(b). $2 \mid r$, $3 \nmid r$; then $2y_2^2 = p_N(Q_r(a))$ with $Q_r(a)$ odd. Thus using [3; Theorem 6] we see that the only possibility is $N = 3$, whence $2y_2^2 = (Q_r(a))^2 - 1$, or since r is even, we have with $b = Q_{(1/2)r}(a)$, $2y_2^2 = (b^2 \pm 2)^2 - 1$, or $2y_2^2 = (b^2 \pm 1)(b^2 \pm 3)$. It is easily seen that the only possibility for these last equations is $b = 1 = Q_{(1/2)r}(a)$, i.e. $a = 1$, $r = 2$, $N = 3$.

(c). $2 \nmid r$, $3 \mid r$; then $2y_2^2 = P_N(Q_r(a))$, where now $Q_r(a)$ is even. Thus Theorem 2 applies and we find that we can only have $N = 4$, $Q_r(a) = 4$, i.e. $a = 1$, $r = 3$, $N = 4$.

(d). $6 \mid r$; then $2y_2^2 = p_N(Q_r(a)) = p_N(x)$ where $x = Q_r(a) = q_{(1/2)r}(Q_2(a))$ as before. Thus Theorem 4 may be used, and we find that we can have only $N = 2$ with $x = Q_r(a) = 18$ or $19{,}602$, i.e. $r = 6$ with $a = 1$ or 5.

Thus in all we have the following solutions to our equation:—

If $a = 1$. Then $r = 1$ gives $N = 3$, $M = 2$ or $N = 3$, $M = 1$ or $N = 6$, $M = 1$; $r = 2$ gives $N = 3$, $M = 1$; $r = 3$ gives $N = 4$, $M = 1$, and $r = 6$ gives $N = 2$, $M = 1$.

If $a = 5$. Then $M = 1$, $N = 2$, $r = 6$.

If $a \neq 1$, $a^2 = 2y_2^2 - 1$, then $r = 1$, $N = 3$, $M = 1$. The other case does not occur since it would require $a^2 = 2y_2^2 - 1$, $a = y_1^2$. But this is impossible for we should have to have $(y_2^2 - 1)^2 = y_2^4 - y_1^4$, and this cannot occur if $a \neq 1$.

This concludes the proof of the theorem.

THEOREM 7. *Let $D = dN^2$ where d is such that $X^2 - dY^2 = -4$ possesses solutions with both X and Y odd; then no one of the four equations $X^2 = DY^4 \pm 1$, $X^2 = DY^4 \pm 4$ possesses more than one solution in positive integers, and between them they have at most two such solutions, the following cases only excepted*

(i) *$D = 5$ when there are in all five solutions, viz. $Y = 1$ for $X^2 = 5Y^4 - 1$, $X^2 = 5Y^4 \pm 4$, $Y = 2$ for $X^2 = 5Y^4 + 1$, $Y = 12$ for $X^2 = 5Y^4 + 4$*

(ii) *$D = 20$ when there are in all three solutions, viz. $Y = 1$ for $X^2 = 20Y^4 - 4$, $Y = 2$ for $X^2 = 20Y^4 + 4$ and $Y = 6$ for $X^2 = 20Y^4 + 1$.*

Proof. We are given that $X^2 - dY^2 = -4$, possesses solutions with both X and Y odd, and so if $X = a$, $Y = b$ is the fundamental solution it is easily seen that both a and b must be odd, for the general solution is given by $X + Yd^{1/2} = 2\{(a + bd^{1/2})/2\}^{2n-1}$. Then we find without difficulty that, considering only positive values, the general solution of $X^2 - dY^2 = -4$ is $Y = bP_{2n-1}(a)$, the general solution of $X^2 - dY^2 = 4$ is $Y = bP_{2n}(a)$, the general solution of $X^2 - dY^2 = -1$ is $Y = (1/2)bP_{6n-3}(a)$, the general solution of $X^2 - dY^2 = 1$ is $Y = (1/2)bP_{6n}(a)$.

Consider first $X^2 - DY^4 = -4$; by the above remarks, we see that for a solution we must have $NY^2 = bP_{2n-1}(a)$, and so if there were two solutions we should have, with $m \neq n$, $P_{2m-1}(a)P_{2n-1}(a) = y^2$, but that is impossible by Theorem 5. The same applies to the equation $X^2 = DY^4 - 1$.

Similarly for $X^2 - dY^4 = 4$ we find that for a solution we must have $NY^2 = bP_{2n}(a)$, and so two different solutions require $m \neq n$ and $P_{2m}(a)P_{2n}(a) = y^2$. Theorem 5 shows that this can occur only for $a = 1$, $2m = 12$, $2n = 2$, from which we find $d = 5$, $NY^2 = 1$ and 144 and so we get only $D = 5$, $Y = 1$ and 12. Similarly we find that $X^2 = DY^4 + 1$ never has more than one solution.

This shows that no one of the equations has more than one solution ($D \neq 5$); to complete the proof we must consider how often two different equations of the set can have solutions. Whenever this occurs we find that $P_r(a)P_s(a) = y^2$ or $2y^2$. These cases are all easily identified using Theorems 5 and 6, and we obtain the required result; for we see that unless $a = 1$, there are in all at most two solutions and examination of $a = 1$ yields all the exceptional cases.

This concludes the proof. In just the same way as above, we may prove the following three results, the proofs of which are omitted.

THEOREM 8. *The equation* $y^2 = p_m(a)p_n(a)$ *where* a *is odd,* $a \geqq 3$ *and* $m \geqq n > 0$ *has only the trivial solution* $m = n$ *except for* $a = 3$, $m = 6$, $n = 1$ *and for* $a = A^2$, $m = 2$, $n = 1$.

THEOREM 9. *The equation* $2y^2 = p_m(a)p_n(a)$ *where* a *is odd,* $a \geqq 3$, *and* $m > n > 0$ *has no solutions except for the following cases*

$$a = 3,\ m = 6,\ n = 3;\ a = 27,\ m = 6,\ n = 3 \text{ and } a^2 = 2A^2+1,\ m = 3,\ n = 1 .$$

THEOREM 10. *Let* $D = dN^2$ *where* d *is such that* $X^2 - dY^2 = 4$ *possesses solutions with both* X *and* Y *odd, although the equation* $X^2 - dY^2 = -4$ *does not; then the equations* $X^2 = DY^4 + 1$ *and* $X^2 = DY^4 + 4$ *possess between them at most two solutions in positive integers, the former having at most one such solution.*

It may be seen from the last theorem, that the equation $X^2 =$

$189Y^4+1$ possesses only the solution $X=55$, $Y=2$ in positive integers, although 189 is not a value to which the methods of [2] or [3] apply; similarly for $D=325$, using Theorem 7, we find that $X^2=325Y^4+1$ has only the solution $Y=6$, and $X^2=325Y^4-1$ has only the solution $Y=1$, while $X^2=325Y^4\pm 4$ have no positive solutions, although again 325 is not a value of D to which the methods of [2] or [3] apply.

We now prove similar results for $Q_n(a)$ and $q_n(a)$, where we suppose throughout that a is odd, and in the case of the latter that $a \geqq 3$. We recall that in the reference [2] we designated $Q_n(a)$ by v_n, and in [3] we designated $q_n(a)$ by v_n. Where no confusion arises, we shall write simply Q_n and q_n.

LEMMA 1. $(Q_m, Q_n) = 2^i x$, *where*

$$\begin{aligned} x &= Q_r \quad \textit{if} \quad r=(m,n) \textit{ and } m/r,\, n/r \textit{ are both odd}\,, \\ &= 1\,, \quad \textit{otherwise}\,; \\ \textit{and} \quad i &= 0 \quad \textit{unless} \quad x = 1,\, 3\,|\, r \\ &= 1 \quad \textit{if} \qquad x=1,\, 3\,|\, r\,. \end{aligned}$$

Proof. If $X=(Q_m, Q_n)$ then since $P_{2t}=P_tQ_t$, we find that X divides $(P_{2m}, P_{2n}) = P_{(2m,2n)} = P_{2r} = P_rQ_r$. Now $P_r\,|\,P_m$ and so no odd factor of P_r divides Q_m in view of (15). Also, if m/r is even we find in view of [2; (19)] that $2Q_m \equiv \pm 4 \pmod{Q_r}$, and so no odd factor of Q_r divides Q_m. Similarly if n/r is even. On the other hand if $M = m/r$ is odd, then $Q_m(a) = Q_M(Q_r(a))$ by (17) if r is odd, and $Q_m(a) = q_M(Q_r(a))$ if r is even by (18), and in either case, $Q_m(a)$ is divisible by $Q_r(a)$. Thus if we define x as in the statement of the lemma, we find that $X=2^i x$ for some suitable i. If $3 \nmid r$, then $2 \nmid X$ and $i=0$. If $6\,|\,r$ then $2\,||\,Q_m$, $2\,||\,Q_n$ and $2\,||\,Q_r$ and so $i=0$ if $x=Q_r$ and $i=1$ if $x=1$. If $r\equiv 3 \pmod 6$, then if $x\neq 1$, $2^2\,|\,Q_r$, $2^2\,||\,Q_m$, $2^2\,||\,Q_n$ and $i=0$, whereas if $x=1$, then one of m and n must be even, and again $i=1$.

In exactly the same way we may prove

LEMMA 2. $(q_m, q_n) = 2^i x$ *where*

$$\begin{aligned} x &= q_r \quad \textit{if} \quad r=(m,n) \textit{ and } m/r,\, n/r \textit{ are both odd}\,, \\ &= 1 \quad \textit{otherwise}\,; \\ \textit{and} \quad i &= 0 \quad \textit{unless} \quad x = 1,\, 3\,|\, r \\ &= 1 \quad \textit{if} \qquad x=1,\, 3\,|\, r\,. \end{aligned}$$

The proof is exactly similar, and is omitted.

LEMMA 3. *$Q_n = ay^2$ implies $n = 1$, except for $a = 1$, $n = 3$.*

Proof. By [2] $a = 1$ occurs only for $n = 1, 3$. In what follows we suppose that $a > 1$. Then $a \mid Q_n$ implies that n is odd.

(i) Suppose $n \equiv 1 \pmod 4$, $n \neq 1$. Then we may write $n = 1 + 2hk$, where h is odd, and $k = 2^R$, $R \geqq 1$. Thus using [2; (23)] we obtain from the equation,

$$\begin{aligned} Q_1 y^2 = ay^2 = Q_n &= Q_{1+2hk} \\ &\equiv -Q_1 \quad \pmod{Q_k} . \end{aligned}$$

Thus in view of Lemma 1, we see that we should have $y^2 \equiv -1 \pmod{Q_k}$ which is impossible, since by [2; (16)] $Q_k \equiv 3 \pmod 4$.

(ii) Suppose $n \equiv 3 \pmod 4$. Then $n = 3$ would give $y^2 = a^2 + 3$, impossible if $a \neq 1$, while if $n \neq 3$ we write $n = 3 + 2hk$ as before, and obtain

$$\begin{aligned} ay^2 &= Q_{3+2hk} \\ &\equiv -Q_3 \quad \pmod{Q_k} , \end{aligned}$$

whence $(a \mid Q_k) = -(Q_3 \mid Q_k)$, which is impossible in view of [2; (27), (28)].
This concludes the proof.

LEMMA 4. *$q_n = ay^2$ implies $n = \pm 1$.*

Proof. As before n must be odd. If $n \equiv 1 \pmod 4$ and $n \neq 1$ then $n = 1 + 2hk$ gives as before

$$ay^2 = q_n \equiv -q_1 \equiv -a \quad \pmod{q_k}$$

which is impossible.

If $n \equiv 3 \pmod 4$, then $q_{-n} = q_n$ in view of [3; (7)] and $-n \equiv 1 \pmod 4$, and the result follows.

LEMMA 5. *$Q_n = 2ay^2$ is impossible, except for $a = 1$ with $n = 0$, $n = 6$.*

Proof. By [2], $a = 1$ gives only $n = 0$, $n = 6$ and so we suppose that $a > 1$. As before $a \mid Q_n$ then implies that n is odd, and $2 \mid Q_n$ implies that $3 \mid n$. Thus $n \equiv 3 \pmod 6$ from which we find that $Q_n \equiv 4 \pmod 8$, which makes $2ay^2 = Q_n$ impossible.

LEMMA 6. *$q_n = 2ay^2$ is impossible for $a > 1$.*

Proof. As before we find $n = 3N$ with N odd, and so

$$2y^2 = \frac{1}{a}q_n \equiv \frac{1}{a}q_3 \pmod 8$$
$$\equiv 6 \pmod 8 ,$$

using [3; (17)], and this is impossible.

THEOREM 11. *The equation $y^2 = Q_m(a)Q_n(a)$ where a is odd and $m \geqq n \geqq 0$ has only the trivial solution $m = n$, except for $a = 1$, $m = 6$, $n = 0$; $a = 1$, $m = 3$, $n = 1$ and $a = 5$, $m = 6$, $n = 0$.*

Proof. In view of Lemma 1, we find three possibilities, where $r = (m, n)$:—

(a) $Q_m(a) = y_1^2$; $Q_n(a) = y_2^2$;

(b) $Q_m(a) = 2y_1^2$; $Q_n(a) = 2y_2^2$;

(c) $Q_m(a) = Q_r(a)y_1^2$; $Q_n(a) = Q_r(a)y_2^2$.

Cases (a) and (b) are easily dealt with, using [2], and we find just the three exceptions stated in the statement of the theorem. Consider case (c).

(i) If $r \equiv \pm 1 \pmod 6$, then write $A = Q_r(a)$ where A is odd, and then in view of (17) we find, where $M = m/r$, $Ay_1^2 = Q_M(A)$. Using Lemma 3, we find that we must have $M = 1$, or $m = r = n$ (similarly) except if $A = 1$, when we find also $m = 3r$, $n = r$ with $A = 1 = Q_r(a)$. But this is possible only for $a = r = 1$, a case we have dealt with already.

(ii) If $r \equiv \pm 2 \pmod 6$, then similarly $A = Q_r(a)$ is odd and using (18) we find $Ay_1^2 = q_M(A)$ which in view of Lemma 4 yields only $m = r = n$.

(iii) If $3 | r$, then $M = m/r$ is odd. Suppose first that $M \equiv 1 \pmod 4$. Then if $M \neq 1$, we find that $m = r + 2hk$ where h is odd and $k = 2^R$. Thus as before we find

$$Q_r(a)y_1^2 = Q_m(a) \equiv -Q_r(a) \pmod{Q_k(a)} .$$

But by Lemma 1, $(Q_r, Q_k) = 1$, and again we see that this is impossible.

If r is even, and $M \equiv 3 \pmod 4$, we find that m is even and then in view of [2; (7)] $Q_{-m}(a) = Q_m(a)$ where now $-m/r \equiv 1 \pmod 4$, and the result follows from the last part.

Finally, if r is odd, $3 | r$ and $M \equiv 3 \pmod 4$, we find if $X = Q_r(a)$ that $4 | X$. But then $Xy_1^2 = Q_M(X)$, and then using (8) we obtain

$$\begin{aligned} y_1^2 &= \frac{1}{X} Q_M(X) \\ &\equiv M \qquad (\text{mod } X^2) \, . \end{aligned}$$

Thus $y_1^2 \equiv 3 \pmod 4$, clearly impossible.
This concludes the proof of the theorem.

THEOREM 12. *The equation* $2y^2 = Q_m(a)Q_n(a)$ *where* a *is odd and* $m > n \geqq 0$, *has no solutions, except for*

$$\begin{aligned} &a = 1 \quad \textit{with} \quad m, n = 3, 0 \ \textit{or} \ 6, 1 \ \textit{or} \ 6, 3; \ \textit{or} \ 1, 0 \, ; \\ &a = 3 \quad \textit{with} \quad m, n = 3, 0 \\ &a = A^2 \quad \textit{with} \quad m, n = 1, 0 \, . \end{aligned}$$

Proof. In view of Lemma 1, $2y^2 = Q_m(a)Q_n(a)$ implies

$$\begin{aligned} &\textit{either} \quad Q_m(a) = y_1^2; \, Q_n(a) = 2y_2^2 \, , \quad \text{or vice-versa} \, ; \\ &\textit{or} \qquad Q_m(a) = Q_r(a)y_1^2; \, Q_n(a) = 2Q_r(a)y_2^2 \quad \text{or vice-versa} \, . \end{aligned}$$

The former gives the exceptions of the theorem, using [2] with [1]. We consider therefore the latter.

As we have seen in the proof of the last theorem, $Q_m(a) = Q_r(a)y_1^2$ is possible only for $m = r$, except for $r = a = 1$, $m = 3$ and again this gives only some of the exceptions found already.

Consider therefore $Q_n(a) = 2Q_r(a)y_2^2$, where $N = n/r$ is odd, $Q_r(a) \neq 1$.

(i) If $r \equiv \pm 1 \pmod 6$, then $A = Q_r(a)$ yields as before $Q_N(A) = 2Ay_2^2$, impossible by Lemma 5, since $A = Q_r(a) \neq 1$.

(ii) If $r \equiv \pm 2 \pmod 6$, then $A = Q_r(a)$ yields as before $q_N(A) = 2Ay_2^2$, impossible in view of Lemma 6.

(iii) If $3 \mid r$, then we find since $N = n/r$ is odd that $Q_r(a)$ and $Q_n(a)$ are divisible by the same power of 2, and so $Q_n(a) = 2Q_r(a)y_2^2$ is impossible in this case.

This concludes the proof.

THEOREM 13. *Let* d *be such that* $X^2 - dY^2 = -4$ *has solutions with both* X *and* Y *odd. Then for any positive integer* N, *the four equations* $N^2X^4 - dY^2 = \pm 1, \pm 4$ *have between them at most one solution in positive integers* X, Y, *with the two exceptions*

(i) $d = 5$, $N = 1$ *when we obtain precisely three solutions, viz.*

$X = 1$ or 2 for $X^4 - 5Y^2 = -4$ and $X = 3$ for $X^4 - 5Y^2 = 1$

(ii) *$d = 5, N = 2$ when we obtain precisely two solutions, viz. $X = 1$ for $4X^4 - 5Y^2 = -1$ and $X = 3$ for $4X^4 - 5Y^2 = 4$.*

Proof. Since $X^2 - dY^2 = -4$ has solutions with both X and Y odd, it follows that $d \equiv 5 \pmod 8$, and that every factor of $d \equiv 1 \pmod 4$. Thus d has at least one prime factor p, with $p \equiv 5 \pmod 8$. If $p \mid N$, then clearly no one of the equations $N^2X^4 - dY^2 = \pm 1, \pm 4$ has a solution. If $p \nmid N$, then since both -1 and 4 are quartic-non-residues modulo p we see that it is impossible that one equation of the pair $N^2X^4 - dY^2 = 1, -4$ and one of the pair $N^2X^4 - dY^2 = -1, 4$ should have solutions.

As in the proof of Theorem 7, we find that the general solution of $X^2 - dY^2 = 4$ is given by $X = Q_{2n}(a)$, $Y = bP_{2n}(a)$ (with analogous results for $X^2 - dY^2 = -4, 1, -1$), and so if any one of the four equations had more than one solution we should obtain $Q_m(a)Q_n(a) = y^2$ with $m > n > 0$, if we restrict our attention to positive solutions for both X and Y. In view of Theorem 11, this cannot occur, with the sole exception of $a = 1$, $m = 3$, $n = 1$, when we find $d = 5$, $N = 1$ with $X = 1$ or 2 satisfying $X^4 - 5Y^2 = -4$. Similarly, if both equations of a pair have solutions, then we should have $Q_m(a)Q_n(a) = 2y^2$ with $m > n > 0$, and in view of Theorem 12, this occurs only for $a = 1$, with $m = 6$ and $n = 1$ or 3. These easily yield the remaining exceptions, mentioned in the statement of the theorem. This concludes the proof.

In exactly the same way we may prove

THEOREM 14. *The equation $y^2 = q_m(a)q_n(a)$, where $a \geqq 3$, and a is odd, and $m \geqq n \geqq 0$ has only the trivial solution $m = n$, except for $a = 3$ or 27 when also $m = 3$, $n = 0$.*

THEOREM 15. *The equation $2y^2 = q_m(a)q_n(a)$, where $a \geqq 3$, and a is odd, and $m > n \geqq 0$ has no solutions except in the case $a = A^2$, when only $m = 1$, $n = 0$.*

THEOREM 16. *Suppose that d is such that $X^2 - dY^2 = 4$ has a solution with both X and Y odd, but that $X^2 - dY^2 = -4$ does not; then for any positive integer N, the equations $N^2X^4 - dY^2 = 1$ and $N^2Y^4 - dY^2 = 4$ have between them at most one solution in positive integers.*

The details of the proofs are similar to the previous ones, and are omitted.

We now consider for a given odd a and given N the problem of determining all positive integers n such that $P_n(a) = Ny^2$. Without loss of generality we may assume that N is square-free. The cases $N = 1, 2$ have been completely dealt with in [2] and so we assume that $N \geqq 3$. In view of Theorem 5 we see that there is at most one such value of n, with the sole exception $N = 10$, $a = 3$ when we can have $n = 3$ or $n = 6$. In other cases the problem of determining the single value of n, if it exists, remains. For convenience we treat separately $P_n(a) = Ny^2$ and $P_n(a) = 2Ny^2$ where N is odd, square-free, and $N \neq 1$.

We see that in view of (3) the residues modulo N of the sequence $P_n(a)$ form a periodic sequence (with period $\leqq N^2$) and since $P_0(a) = 0$ there exists a least positive integer $\rho = \rho(N, a)$, say, such that $N | P_\rho(a)$. It is then easily seen that $N | P_n(a)$ if and only if $\rho | n$.

(a) *Suppose* $\rho \equiv \pm 1 \pmod 6$.

We have using (13) that with $d = (a^2 + 4)N^2$, the equation $X^2 - dy^2 = -4$ is satisfied by $X = A = Q_\rho(a)$ and $Y = B = N^{-1}P_\rho(a)$. Since $3 \nmid \rho$, both A and B are odd and since the general solution of $X^2 - (a^2 + 4)Y^2 = -4$ is given by $X = Q_{2n-1}(a)$, $Y = P_{2n-1}(a)$, it is clear that $A + Bd^{1/2}$ is the fundamental solution of $X^2 - dY^2 = -4$. Thus the methods of [2] apply for this value of d, and we find in the notation employed there that, in view of (7) and (8)

$$\begin{aligned} d^{1/2}u_r &= \left\{\frac{A + Bd^{1/2}}{2}\right\}^r - \left\{\frac{A - Bd^{1/2}}{2}\right\}^r \\ &= \left\{\frac{Q_\rho(a) + (a^2 + 4)^{1/2}P_\rho(a)}{2}\right\}^r - \left\{\frac{Q_\rho(a) - (a^2 + 4)^{1/2}P_\rho(a)}{2}\right\}^r \\ &= \left\{\frac{a + (a^2 + 4)^{1/2}}{2}\right\}^{r\rho} - \left\{\frac{a - (a^2 + 4)^{1/2}}{2}\right\}^{r\rho} \\ &= (a^2 + 4)^{1/2}P_{r\rho}(a) . \end{aligned}$$

Thus $P_{r\rho}(a) = Nu_r$. Accordingly we see that $P_{r\rho}(a) = Ny^2$ implies $u_r = y^2$, and using [2; Theorem 3] this is possible for positive r only with $r = 1, 2$ and for $d = 5$ with $r = 12$. But $d = 5$ is impossible since $N \neq 1$. Also $r = 2$ would require $A = Q_\rho(a)$ to be a square, and using [2; Theorem 7] this would require $\rho \leqq 3$, that is $\rho = 1$. But $\rho = 1$ is impossible, since then $N \nmid P_\rho(a)$.

Similarly $P_n(a) = 2Ny^2$ implies $n = r\rho$ with $u_r = 2y^2$. Using [2; Theorem 4] we see that since $d \neq 5$, we need consider only $r = 3$. But this too is impossible, for we should obtain $2y^2 = B(A^2 + 1)$. Since $A^2 - dB^2 = -4$, $A^2 + 1 \equiv -3 \pmod B$ and so since $3 \nmid (A^2 + 1)$ we should have $A^2 + 1 = 2y_1^2$; $B = y_2^2$. But then $P_\rho(a) = NB = Ny_2^2$, whence $P_\rho(a)P_{3\rho}(a) = 2y_3^2$, impossible in view of Theorem 6, since in this case $\rho \geqq 5$.

Thus in case (a) $P_n(a) = Ny^2$ *can occur only for* $n = \rho$;
$P_n(a) = 2Ny^2$ *cannot occur at all for* $n > 0$.

(b) *Suppose* $\rho \equiv \pm 2 \pmod 6$.

We now find in analogous fashion that if $d = (a^2 + 4)N^2$, then $X^2 - dY^2 = -4$ has no solution, but that the fundamental solution of $X^2 - dY^2 = 4$ is $A = Q_\rho(a)$, $B = N^{-1}P_\rho(a)$ with both A and B odd. Thus we use the notation and methods of [3], finding as before that $P_{r\rho}(a) = Nu_r$ and so $P_{r\rho}(a) = Ny^2$ implies $u_r = y^2$. For positive r this can occur [3; Theorem 3] only for $r = 1$, 2 or 3. But $r = 2$ is impossible for it would require $y^2 = N^{-1}P_{2\rho}(a) = (N^{-1}P_\rho(a))Q_\rho(a)$ whence $Q_\rho(a) = y_1^2$, impossible for even ρ by [2; Theorem 1]. Also $r = 3$ would require $y^2 = u_3 = B(A^2 - 1)$, whence $B = 3y_1^2$; $A^2 - 1 = 3y_2^2$. Now since A is odd, $A^2 - 1 \equiv 0 \pmod 8$ and so we must have $A^2 \equiv 1 \pmod{16}$. Thus $A \equiv \pm 1 \pmod 8$ and this leads to $\rho \equiv 0 \pmod 4$. Thus if $c = Q_{(1/4)\rho}(a)$ we find using [2; (11)] that

$$\begin{aligned} 3y_2^2 &= \{Q_{(1/2)\rho}(a))^2 - 2\}^2 - 1 \\ &= (Q^2_{(1/2)\rho} - 1)(Q^2_{(1/2)\rho} - 3) \\ &= ((c^2 \pm 2)^2 - 1)((c^2 \pm 2)^2 - 3) \\ &= (c^4 \pm 4c^2 + 3)(c^4 \pm 4c^2 + 1) , \end{aligned}$$

where c is odd. Now both expressions in brackets are positive except for $c = 1$; otherwise since $c^4 \pm 4c^2 + 1 \equiv 6 \pmod 8$ we must have

$$\begin{aligned} c^4 \pm 4c^2 + 1 &= 6y_3^2 \\ c^4 \pm 4c^2 + 3 &= 2y_4^2 . \end{aligned}$$

Now we reject the lower sign since $3 \mid (c^4 - 4c^2)$ for every c, contradicting the former. The upper sign gives

$$\frac{c^2 + 1}{2}(c^2 + 3) = y_4^2 .$$

This requires $c^2 + 3 = y_5^2$, and this is possible only for $c = 1$. But $c = 1 = Q_{(1/4)\rho}(a)$ can occur only for $a = 1$, $\rho = 4$. But this would require $N = 3$, since $P_4(1) = 3$, but $P_{12}(1) = 144 \neq 3y^2$.

Finally, $P_{r\rho}(a) = 2Ny^2$ implies $u_r = 2y^2$, possible in view of [3; Theorem 4] only for $r = 3$, with $B = y_1^2$. But then $P_\rho(a) = NB = Ny_1^2$. Thus $P_\rho(a)P_{3\rho}(a) = 2y_2^2$, possible in view of Theorem 6 only for $a = 1$, $\rho = 2$. But again this cannot occur since $P_2(1) = 1$.

Thus in case (b) , $P_n(a) = Ny^2$ *can occur only for* $n = \rho$; $P_n(a) = 2Ny^2$ *is impossible for* $n > 0$.

(c) *Suppose* $\rho \equiv 3 \pmod 6$.

Then $P_{r\rho}(a) = Ny^2$ compels r to be even. For if r is odd, then $2 \mid P_{r\rho}(a)$, $4 \nmid P_{r\rho}(a)$. Thus we write $r = 2s$, and then

$$y^2 = N^{-1}P_{2s\rho}(a) = \{N^{-1}P_{s\rho}(a)\}\{Q_{s\rho}(a)\} .$$

Thus in view of (15) we have

$$\begin{array}{ll} \textit{either} & P_{s\rho}(a) = Ny_1^2;\ Q_{s\rho}(a) = y_2^2 \\ \textit{or} & P_{s\rho}(a) = 2Ny_1^2;\ Q_{s\rho}(a) = 2y_2^2 . \end{array}$$

Now using [2; Theorem 7] we find that the former requires $s = 3$, with $a = 1$ or 3, but then $P_{s\rho}(a) = 2$ or 10, neither of which gives a value for N. Using [2; Theorem 8], with [1] gives $s\rho = 6$ with $a = 1$ or 5, whence $2Ny_1^2 = 8$ or 3640. The former gives no value, the latter $\rho = 3$, $r = 4$, $a = 5$, $N = 455$; but $455 \nmid P_3(5)$ and so we find that this cannot occur.

Thus in case (c) , $P_n(a) = Ny^2$ *cannot occur for* $n > 0$.

Unfortunately, there does not seem to be a similar method available for handling $P_n(a) = 2Ny^2$ in this case.

(d) *Suppose* $\rho \equiv 0 \pmod 6$.

This case is slightly more complicated; suppose $2^t \| \rho$. Then it may be shown that $2^{t+2} \| P_\rho(a)$ and so if t is odd, we find that $Ny^2 = P_n(a)$ implies $n = r\rho$ with r even, and then just as in the above case we find no value for $n > 0$, except in the case $a = 5$, $\rho = 6$, $N = 455$, $n = 12$. On the other hand, if t is even, we find that $2Ny^2 = P_n(a)$ implies $n = r\rho$ with r even, and then there is no value for $n > 0$.

Thus in case (d), *if* $2^{2t} \| \rho$, *then* $P_n(a) = 2Ny^2$ *has no solution, and if* $2^{2t+1} \| \rho$, *then* $P_n(a) = Ny^2$ *has no solution, except in the single case* $a = 5$, $N = 455$, $n = 12$, *all for* $n > 0$.

We see however, that in the cases in which $3 \mid \rho(N, a)$, we have not succeeded in determining possible values of n. This problem remains open. A similar situation exists for equations of the type $p_n(a) = Ny^2$.

In conclusion, we observe that as far as Theorems 1–4 are concerned, although the method applies to infinite sets of values of x in each case, many values are not covered; thus considering values $< 6{,}000$ the only values covered are 4, 36, 76, 140, 364, 756, 1364, 2236, 3420 and 4964 in the case of Theorems 1 and 2, and 18, 110, 322, 702, 1298, 2158, 3330, 4862 and 5778 in the case of Theorems 3 and 4. For such values it is also clear that a method similar to that used in [4] will be available for handling *any* sequence of integers satisfying a recurrence relationship of the form (3) or (5) respectively.

References

1. R. T. Bumby, *The diophantine equation* $3x^4 - 2y^2 = 1$, Math. Scand., **21** (1967), 144-148.
2. J. H. E. Cohn, *Eight diophantine equations*, Proc. London Math. Soc. (3) **16** (1966), 153-166.
3. ———, *Five diophantine equations*, Math. Scand., **21** (1967), 61-70.
4. ———, *Some quartic diophantine equations*, Pacific J. Math., 26 (1968) 233-243.
5. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$., Avh. Norske Vid. Akad. Oslo I, (1942) Nr. 5.

Received March 15, 1971.

ROYAL HOLLOWAY COLLEGE
ENGLEFIELD GREEN, SURREY