A THESIS

submitted for the Degree of

DOCTOR OF PHILOSOPHY

in the

UNIVERSITY OF LONDON

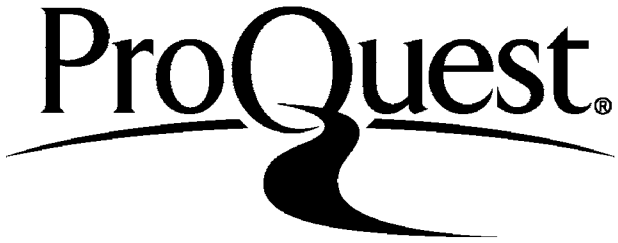
by

Vivienne M.Stapley

entitled

SQUARES IN CERTAIN RECURRENT SEQUENCES AND SOME DIOPHANTINE EQUATIONS.

Royal Holloway College July 1971.



ABSTRACT.

The object of this thesis is to solve, in integers X and Y, various equations of the form $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dY^4 = \pm 1, \pm 4$; $N^2X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dN^2Y^4 = \pm 1, \pm 4$, where d and N are given square free integers.

The work stems from two papers by J.H.E.Cohn in which the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$ are solved for certain values of d.

It is well known that the solutions of $X^2 - dY^2 = 4$, and those of $X^2 - dY^2 = -4$ where such solutions exist, may be expressed in terms of the least positive solutions of these equations. Solutions of the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$ may now be sought among those of $X^2 - dY^2 = \pm 1, \pm 4$.

Extensive work in this direction has been done by W.Ljunggren working in the quadratic field $R(d^{\frac{1}{2}})$ and other allied algebraic fields. His methods are powerful but deep and complicated.

It is possible to show that the solutions of the equations $X^2 - dY^2 = \pm 4$ form sequences which satisfy a three-term recurrence relation. By applying the elementary theory of quadratic residues to these equations Cohn has solved the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$ for those d for which either of the equations $X^2 - dY^2 = \pm 4$ has solutions (X,Y) for which X and Y are both odd.

This thesis extends Cohn's work, using similar methods, to solve the equations $N^2X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dN^2Y^4 = \pm 1, \pm 4$ for the same values of d as above and any given integer N.

A few limited results are given for other values of d.

L.J.Mordell has given simple conditions under which the equation $X^2 - dY^4 = 1$ can have no solutions. A theorem of a similar type concerning the equations $X^4 - dY^2 = 1, 4$ is proved.

Finally the results proved in this thesis are compared with those of Cohn, Ljunggren and Mordell.

ACKNOWLEDGEMENTS.

I should like to take this opportunity to express my thanks to my supervisor, Dr. J.H.E. Cohn, for his help and encouragement. I am grateful to the Department of Pure Mathematics in the University of St.Andrews for arranging my teaching responsibilities to allow time for completing this work and to the Science Research Council for a Research Studentship.

CONTENTS.

	Page
Notation	6
Introduction	7
Chapter 1	17
Chapter 2	72
Chapter 3	79
Chapter 4	124
Chapter 5	132
References	158

NOTATION.

The following standard notation is used:

(m,n)	denotes	the highest common factor of m and n.
$m \mid n$	denotes	'm divides n'.
$m \nmid n$	denotes	'm does not divide n'.
$\Longleftrightarrow$	denotes	' implies and is implied by '.
(R / S)	denotes	the Jacobi symbol for R and S.

The properties of this last symbol are explained in the Introduction, on page 13.

INTRODUCTION.

The work in this thesis stems from two papers, (2, 4), by J.H.E.Cohn, which are concerned with the solution, in integers X and Y, of the Diophantine Equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$.

It is a long-established fact that the equation $X^2 - dY^2 = 1$ has infinitely many solutions, in integers X and Y, for every non-square integer $d>0$. The first published proof of this was given, around 1766, by Lagrange using the theory of continued fractions. Many other proofs have been given since. See, for example, (14).

Thus the equation $X^2 - dY^2 = 4$ always has solutions, since if (x,y) is a solution of $X^2 - dY^2 = 1$, (2x, 2y) is a solution of $X^2 - dY^2 = 4$. For brevity we shall refer to $X + Yd^{\frac{1}{2}}$, as well as (X,Y) as a solution of $X^2 - dY^2 = 4$. Such a solution will be called positive if $X > 0$, $Y > 0$. The positive solutions may be ordered by the size of X, or, what is the same thing, by the size of $X + Yd^{\frac{1}{2}}$, since if $X_1 + Y_1 d^{\frac{1}{2}}$ and $X_2 + Y_2 d^{\frac{1}{2}}$ are positive solutions of $X^2 - dY^2 = 4$ for which $X_1 > X_2$, then

$$X_1 + Y_1 d^{\frac{1}{2}} > X_2 + Y_2 d^{\frac{1}{2}}$$

and vice versa.

Now it is easily shown that, if $a + bd^{\frac{1}{2}}$ is the least positive solution of $X^2 - dY^2 = 4$, then the general solution is given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^n$$

where n is any integer. See, for example (6). Because of

this fact, the least positive solution is often called the fundamental solution, a convention which we adopt in this thesis.

Unlike the equation $X^2 - dY^2 = 1$, the equation $X^2 - dY^2 = -1$ does not have solutions, in integers X and Y, for all non-square values of $d>0$. For example, it is easily seen that if $X^2 - dY^2 = -1$, then any factor of d is congruent to 1, 2, or 5 (mod 8.). Even this condition is not sufficient as, for example, the equation $X^2 - 34Y^2 = -1$ has no solutions in integers X and Y. See (15). However, if the equation $X^2 - dY^2 = -1$ has solutions, the situation is very similar to that described above. For then, clearly, the equation $X^2 - dY^2 = -4$ has solutions and we can show that, if $a + bd^{\frac{1}{2}}$ is the fundamental solution of $X^2 - dY^2 = -4$, then the general solution is given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^{2n-1}$$

where n is any integer. We can also show that, for these values of d, the general solution of $X^2 - dY^2 = 4$ is given by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^{2n}$$

i.e. in this case the fundamental solution of $X^2 - dY^2 = 4$ is given by $2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^2$

Now the equations $X^2 - dY^2 = \pm 1, \pm 4$ are closely connected with the real quadratic field $R(d^{\frac{1}{2}})$, i.e. the field consisting of all the numbers of the form

$$r + sd^{\frac{1}{2}}$$

where r and s are rational numbers, positive, negative or zero. Each of these numbers, where $s \neq 0$, is a zero of a unique quadratic polynomial with relatively prime integral coefficients, the leading coefficient being positive. If the leading coefficient is 1, the corresponding number is said to be an integer of the field. Starting with this definition of integer it is possible to construct an arithmetic very similar to that of the rational integers. We denote by $R[d^{\frac{1}{2}}]$ the set of all integers of $R(d^{\frac{1}{2}})$. If α, β and $\frac{\alpha}{\beta}$ are in $R[d^{\frac{1}{2}}]$ we say β divides α and write $\beta \mid \alpha$. If $\frac{\alpha}{\beta} \mid 1$, α is called a unit of $R[d^{\frac{1}{2}}]$. If $\alpha = a + bd^{\frac{1}{2}}$, the norm of α, $N\alpha$, is the product of α with its algebraic congugate $\bar{\alpha} = a - bd^{\frac{1}{2}}$, i.e. $N\alpha = a^2 - db^2$. It is easily shown that α is a unit of $R[d^{\frac{1}{2}}]$ if and only if $N\alpha = \pm 1$. Since it can be shown that $a + bd^{\frac{1}{2}}$ is a quadratic integer if and only if a and b are rational integers, (or, in the case of $d \equiv 1 \pmod 4$ a and b may be both half odd integers) clearly the units of $F[d^{\frac{1}{2}}]$ are given by the solutions of

$$X^2 - dY^2 = \pm 1, \pm 4.$$

This line of approach was used by Ljunggren, in (7,9,10), to find solutions of the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$. Working in $R[d^{\frac{1}{2}}]$ and other allied algebraic fields, he used the known properties of the units to obtain upper bounds for the number of solutions of the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = 1, \pm 4$. He also found upper bounds for the number of solutions of $X^2 - dY^4 = -1$ for large classes of values of d. In each case he gave a method for finding solutions where they exist.

His methods are very powerful but very complicated and the methods for finding solutions in a given case involve a great deal of computation. It is, therefore, of interest to look for more elementary methods of proving his results, and shorter ways of obtaining solutions in given numerical examples.

In 1964 Mordell gave some simple conditions for d under which the equation $X^2 - dY^4 = 1$ can have no solutions other than (1,0). See (13). In particular, he showed that the equation $X^2 - pY^4 = 1$ has only this solution if p is an odd prime, $p \equiv 5, 9$ or $13 \pmod{16}$, $p \neq 5$. This work was extended by Ljunggren in 1966 to include the case $p \equiv 1 \pmod{16}$. See (12). In this paper Ljunggren also proved that the equation $X^4 - pY^2 = 1$ has no non-trivial solutions if p is an odd prime, $p \neq 5$ or 29. If $p = 5$ or 29 there is just one non-trivial solution in each case.

These two papers used only elementary methods except that they both made use of the fact that the only solutions of the equation

$$X^2 - 2Y^4 = -1$$

are $(X,Y) = (1,1)$ and $(239,13)$. This result was proved by Ljunggren in (10), and the proof is very long and difficult.

In 1966 Cohn published (2) in which equations of the form $X^2 - dY^4 = \pm 1, \pm 4$ and $X^4 - dY^2 = \pm 1, \pm 4$, for certain values of d, were solved using elementary methods - although again it should be noted, (3), that a result from Ljunggren's work, in (7), was needed to deal with one special case.

The d dealt with were those for which the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. In a later paper, (4), Cohn dealt with the equations

$X^4 - dY^2 = 1, 4$ and $X^2 - dY^4 = 1, 4$ for those d for which the equation $X^2 - dY^2 = -4$ has no solutions, but the equation $X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd.

These papers do not cover all the cases dealt with by Ljunggren, but the proofs are shorter and simpler and give a neater method for finding solutions where they exist.

This thesis extends Cohn's work to solve equations of the form $X^2 - dN^2Y^4 = \pm 1, \pm 4$ and $N^2X^4 - dY^2 = \pm 1, \pm 4$ for the same d as those considered in (2, 4). We also obtain one or two results for the case when the equations $X^2 - dY^2 = \pm 4$ have only solutions (X,Y) for which X and Y are both even but the method has limited application in this direction.

Suppose that the equation $X^2 - dY^2 = -4$ has solutions. Let $a + bd^{\frac{1}{2}}$ be the fundamental solution and denote by $(Q_{2n+1}(a), bP_{2n+1}(a))$ the general solution given by

$$Q_{2n+1}(a) + bP_{2n+1}(a)d^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^{2n+1}$$

Then the solutions of $X^2 - dY^2 = 4$ are given by $(Q_{2n}(a), bP_{2n}(a))$ where $$Q_{2n}(a) + bP_{2n}(a)d^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^{2n}$$

Clearly

$$Q_n(a) - bP_n(a)d^{\frac{1}{2}} = 2\left(\frac{a - bd^{\frac{1}{2}}}{2}\right)^{n}$$

for all integers n. Let $\alpha = \frac{1}{2}(a + bd^{\frac{1}{2}})$, $\beta = \frac{1}{2}(a - bd^{\frac{1}{2}})$. Then

$$Q_n(a) = \alpha^n + \beta^n$$

$$P_n(a) = \frac{1}{bd^{\frac{1}{2}}}(\alpha^n - \beta^n)$$

Using these formulae we can show that the sequences $\{Q_n(a)\}$ and $\{P_n(a)\}$ both satisfy a three-term recurrence relation of the form

$$Z_{n+1} = aZ_n + Z_{n-1}$$

Clearly, therefore, the sequences $\{NQ_n(a)\}$ and $\{NP_n(a)\}$ satisfy the same relation for all integers N.

If the equation $X^2 - dY^2 = -4$ has no solutions, let $a + bd^{\frac{1}{2}}$ be the fundamental solution of the equation $X^2 - dY^2 = 4$. Denote by $(q_n(a), bp_n(a))$ the general solution given by

$$q_n(a) + bp_n(a)\, d^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^n$$

Let $\alpha = \frac{1}{2}(a + bd^{\frac{1}{2}})$, $\beta = \frac{1}{2}(a - bd^{\frac{1}{2}})$ as before. Then clearly

$$q_n(a) = \alpha^n + \beta^n$$

$$p_n(a) = \frac{1}{bd^{\frac{1}{2}}}\,(\alpha^n - \beta^n)$$

and we can show that for all integers N, the sequences $\{Nq_n(a)\}$ and $\{Np_n(a)\}$ satisfy a three-term recurrence relation of the form

$$Z_{n+1} = aZ_n - Z_{n-1}.$$

The main part of this thesis is concerned with proving that in many cases only a finite number of specified terms of these sequences can be squares. The method used is based on the following simple reasoning.

For any integers R and $T = S^2$, the congruence

$$x^2 \equiv T \pmod{R}$$

is soluble since $R \mid S^2 - T = 0$. Thus if we are given an integer T and can find an integer R such that the congruence

$$x^2 \equiv T \pmod{R}$$

has no solutions, then T is not a square.

Given an integer Z in one of our sequences, therefore, we seek among the terms of that and the related sequences for an integer R such that the congruence

$$x^2 \equiv Z \pmod{R}$$

is insoluble. In the cases where the fundamental solution $a + bd^{\frac{1}{2}}$ is such that a and b are odd this process is successful and we obtain the desired results. If a and b are even, however, except in a few cases the method breaks down and the results are inconclusive.

To simplify the manipulation we introduce the Legendre symbol and the allied Jacobi symbol.

If the congruence

$$x^2 \equiv T \pmod{R}$$

is soluble, we say that T is a quadratic residue of R. If not, we say that T is a quadratic non-residue of R. The Legendre symbol, (T / p), is defined for all odd primes p and integers T such that $(T,p)=1$ by

$(T / p) = 1$ if T is a quadratic residue of p;

$(T / p) = -1$ if T is a quadratic non-residue of p.

The Legendre symbol can be shown to have the following properties:

(i) $(ST / p) = (S / p)\,(T / p)$.

(ii) If $S \equiv T \pmod{p}$ then $(S / p) = (T / p)$.

(iii) $(T^2 / p) = 1$ if $(T,p) = 1$.

(iv) $(-1 / p) = (-1)^{\frac{1}{2}(p-1)}$.

(v) $(2 / p) = (-1)^{\frac{1}{8}(p^2-1)}$.

(vi) If p and q are both primes, then $(p / q)(q / p) = (-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)}$.

The Jacobi symbol, (T / R), is defined for every odd integer R where R is not necessarily prime. It is defined by

$(T / R) = 1$ if $R = 1$;

$(T / R) = (T / p_1)(T / p_2) \cdots (T / p_r)$ if $R = p_1 p_2 \cdots p_r$

where $p_1, p_2 \cdots p_r$ are primes.

The Jacobi symbol has properties analogous to properties (i) - (vi) given above for the Legendre symbol and

(i)' $(T / RS) = (T / R)(T / S)$.

Also, it is clear that if $(T / R) = -1$ then T is a quadratic non-residue of R. It should be noticed, however, that $(T / R) = 1$ does not necessarily imply that T is a quadratic residue of R, but it is the first mentioned inference which we use.

We deal with the sequences in four groups;

1. $\{Q_n(a)\}$ and $\{P_n(a)\}$ where a is odd;

2. $\{Q_n(a)\}$ and $\{P_n(a)\}$ where a is even;

3. $\{q_n(a)\}$ and $\{p_n(a)\}$ where a is odd;

4. $\{q_n(a)\}$ and $\{p_n(a)\}$ where a is even;

in chapters 1 - 4 respectively.

It is easily shown that the fundamental solution $a + bd^{\frac{1}{2}}$ of $X^2 - dY^2 = -4$ is such that a and b are odd if and only if the equation $X^2 - dY^2 = -4$ has solutions, (X,Y), such that X and Y are both odd. Thus chapter 1 is concerned with the equations $X^2 - dY^2 = \pm 1, \pm 4$ where d is such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y

are both odd. Cohn's paper, (2), dealt with the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$, i.e. $Q_n(a) = X^2$ or $2X^2$ and $bP_n(a) = Y^2$ or $2Y^2$. We set out these results and extend the work to solve the equations $Q_n(a) = Q_m(a)X^2$, $2Q_m(a)X^2$, $P_m(a)X^2$, $2P_m(a)X^2$ and $P_n(a) = P_m(a)Y^2$, $2P_m(a)Y^2$, $Q_m(a)Y^2$, $2Q_m(a)Y^2$. Using these results we then solve the equations $Q_n(a) = NX^2$, $2NX^2$ and $P_n(a) = NY^2$, $2NY^2$, for general square-free values of N.

Similarly, chapter 2 is concerned with the equations $X^2 - dY^2 = \pm 1, \pm 4$ for those d for which the equation $X^2 - dY^2 = -4$ has only solutions, (X,Y), for which X and Y are both even. Here, however, we are able to solve only the equations $Q_{2n}(a) = X^2$, $2X^2$ and $P_{2n}(a) = Y^2$ for those a such that $2 \mid a$, $4 \nmid a$.

If the equation $X^2 - dY^2 = -4$ has no solutions, it is easily shown that the fundamental solution, $a + bd^{\frac{1}{2}}$, of $X^2 - dY^2 = 4$ is such that a and b are both odd if and only if the equation $X^2 - dY^2 = 4$ has solutions, (X,Y), such that X and Y are both odd. Thus chapter 3 is concerned with the equations $X^2 - dY^2 = 1,4$ where d is such that the equation $X^2 - dY^2 = -4$ has no solutions, but the equation $X^2 - dY^2 = 4$ has solutions, (X,Y), such that X and Y are both odd. The equations $X^4 - dY^2 = 1, 4$ and $X^2 - dY^4 = 1, 4$, i.e. $q_n(a) = X^2$, $2X^2$ and $bp_n(a) = Y^2$, $2Y^2$ were solved in (4). Again we set out these results and extend the work to prove results for the functions $q_n(a)$ and $p_n(a)$ analogous to those proved in chapter 1 for the functions $Q_n(a)$ and $P_n(a)$.

In chapter 4 we are concerned with the remaining case of those d for which the equation $X^2 - dY^2 = -4$ has no solutions

and the equation $X^2 - dY^2 = 4$ has only the solutions (X,Y) for which X and Y are both even. The results obtained here, however, are even more limited than those of chapter 2.

In chapter 5 we set out the implications of the results of chapters 1 - 4 for the equations $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dY^4 = \pm 1, \pm 4$; $N^2X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dN^2Y^4 = \pm 1, \pm 4$.

If either of the equations $X^2 - dY^2 = \pm 4$ has solutions, (X,Y), for which X and Y are both odd these equations are dealt with completely and a straightforward method for finding solutions in particular cases is given. It should be noted, however, that this still depends, as do Ljunggren's methods, on finding by trial and error the fundamental solutions of the equations $X^2 - dY^2 = \pm 4$ and for a particular d these may be very large indeed: for example, the fundamental solution of $X^2 - 94Y^2 = 4$ is X = 5,086,590, Y = 442,128.

A few inferences are made in the case where the equations $X^2 - dY^2 = \pm 4$ have only solutions (X,Y) for which X and Y are both even.

We then compare our results with those of Ljunggren in (7 - 11).

Finally we give some conditions for d under which the equations $X^4 - dY^2 = 1, 4$ have no non-trivial solutions and compare our results with the similar work of Ljunggren, Mordell and Cohn in (12), (13) and (5) respectively.

CHAPTER 1.

The object of this thesis is to prove various results concerning the solutions, in integers X and Y, of the equations $X^2 - dY^4 = \pm 1, \pm 4$; $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dN^2Y^4 = \pm 1, \pm 4$ and $N^2X^4 - dY^2 = \pm 1, \pm 4$ where d and N are given square-free integers.

The equations are dealt with in four groups:

1. Those for which the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd.
2. Those for which the equation $X^2 - dY^2 = -4$ has solutions (X,Y) but only such that X and Y are both even.
3. Those for which the equation $X^2 - dY^2 = -4$ has no solutions but the equation $X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd.
4. Those for which the equation $X^2 - dY^2 = -4$ has no solutions and the equation $X^2 - dY^2 = 4$ has only solutions (X,Y) for which X and Y are both even.

If (X,Y) is a solution of either of the equations $X^2 - dY^2 = \pm 4$, then, clearly, if d is odd X and Y have the same parity: if d is even then X is even and hence $dY^2 \equiv 0 \pmod 4$, i.e. Y is even since d is square-free. It is now clear that these four groups exhaust all the possibilities, for it is a well-known fact that the equation $X^2 - dY^2 = 1$, where d is a square-free integer, always has infinitely many solutions in integers X and Y. Thus the equation $X^2 - dY^2 = 4$ must have solutions (X,Y) where X and Y are both even.

Since, if (X,Y) is a solution of either of the equations $X^2 - dY^2 = \pm 4$, X and Y have the same parity, such a solution, from now on, will be referred to as either an "odd" or an "even" solution.

We are able to give quite extensive results for the

equations in groups 1 and 3. It will be seen later that the method used relies heavily upon the fact that the equations $X^2 - dY^2 = \pm 4$ have odd solutions in these cases. In view of this it is of interest to note that if d_1 is such that $X^2 - d_1Y^2 = -4$ has solutions, but no odd ones, then the equation $X^2 - d_1Y^2 = 4$ has no odd solutions either.

For suppose $x_1^2 - d_1 y_1^2 = 4$ where x_1 and y_1 are odd. Then clearly d_1 is odd. Suppose also that $(2x_2)^2 - d_1(2y_2)^2 = -4$, i.e. $x_2^2 - d_1 y_2^2 = -1$. Then since d_1 is odd, x_2 and y_2 are of opposite parity.

Let

$$\xi = x_1x_2 + d_1y_1y_2 : \eta = x_1y_2 + y_1x_2.$$

Then ξ and η are both odd and

$$\xi^2 - d_1\eta^2 = (x_1^2 - d_1y_1^2)(x_2^2 - d_1y_2^2) = -4$$

which contradicts the assumption that $X^2 - d_1Y^2 = -4$ has no odd solutions.

This means that none of the equations in group 2 can be dealt with, even partially, by the method used for the equations in grpup 3 and each group must be dealt with separately.

Some results have been obtained for the equations in groups 2 and 4 but these are very limited.

We now deal with each group separately.

In this chapter we suppose that the equation $X^2 - dY^2 = -4$ has odd solutions.

The results at the beginning of this section, up to and including theorem 1.4, are due to J.H.E.Cohn and are taken from (2).

The general method used is to seek solutions of the equations $X^2 - dY^4 = \pm 1, \pm 4$; $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dN^2Y^4 = \pm 1, \pm 4$ and $N^2X^4 - dY^2 = \pm 1, \pm 4$ among the solutions of $X^2 - dY^2 = \pm 1, \pm 4$.

We begin by establishing some miscellaneous results concerning the solutions of the equations $X^2 - dY^2 = \pm 1, \pm 4$ which we will require later.

Since $X^2 - dY^2 = -4$ has odd solutions, clearly $d = 5 \pmod 8$. If $X = a$, $Y = b$ is the fundamental solution, i.e. the least positive solution, it is a well-known fact that the general solution is given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^{2n-1}$$

See, for example (6).

Thus, since we are assuming that there is a solution for which X and Y are both odd, a and b are also both odd. We write $\alpha = \frac{1}{2}(a + bd^{\frac{1}{2}})$, $\beta = \frac{1}{2}(a - bd^{\frac{1}{2}})$ and have immediately

$$\alpha + \beta = a; \quad \alpha\beta = -1 \tag{1.1}$$

We then define, for all integers n,

$$P_n(a) = \frac{1}{bd^{\frac{1}{2}}}(\alpha^n - \beta^n) \tag{1.2}$$

$$Q_n(a) = \alpha^n + \beta^n \tag{1.3}$$

Then

$$P_{n+2}(a) = \frac{1}{bd^{\frac{1}{2}}}(\alpha^{n+2} - \beta^{n+2})$$

$$= \frac{1}{bd^{\frac{1}{2}}}(\alpha^{n+1} - \beta^{n+1})(\alpha + \beta) + \frac{1}{bd^{\frac{1}{2}}}\alpha\beta(\beta^n - \alpha^n)$$

$$= aP_{n+1}(a) + P_n(a) \text{ from (1.1) and (1.2);}$$

i.e.

$$P_{n+2}(a) = aP_{n+1}(a) + P_n(a) \tag{1.4}$$

Similarly, from (1.1) - (1.3)

$$Q_{n+2}(a) = aQ_{n+1}(a) + Q_n(a) \tag{1.5}$$

$$P_{-n}(a) = (-1)^{n-1} P_n(a) \tag{1.6}$$

$$Q_{-n}(a) = (-1)^n Q_n(a) \tag{1.7}$$

Also, $P_0(a) = 0, P_1(a) = 1, Q_0(a) = 2$ and $Q_1(a) = a$. Thus it is clear that $P_n(a)$ and $Q_n(a)$ are integers for all integers n and moreover positive for positive n. The first few values are:

n	$P_n(a)$	$Q_n(a)$
0	0	2
1	1	a
2	a	$a^2 + 2$
3	$a^2 + 1$	$a^3 + 3a$
4	$a^3 + 2a$	$a^4 + 4a^2 + 2$
5	$a^4 + 3a^2 + 1$	$a^5 + 5a^3 + 5a$
6	$a^5 + 4a^3 + 3a$	$a^6 + 6a^4 + 9a^2 + 2$

Now from (1.2)

$$2P_{m+n}(a) = \frac{2}{bd^{\frac{1}{2}}} (\alpha^{m+n} - \beta^{m+n})$$

$$= \frac{1}{bd^{\frac{1}{2}}} (\alpha^m - \beta^m)(\alpha^n + \beta^n) + \frac{1}{bd^{\frac{1}{2}}} (\alpha^m + \beta^m)(\alpha^n - \beta^n)$$

$$= P_m(a)\, Q_n(a) + Q_m(a)\, P_n(a) \text{ from (1.2) and (1.3)}$$

i.e.

$$2P_{m+n}(a) = P_m(a)\, Q_n(a) + P_n(a)\, Q_m(a) \tag{1.8}$$

Similarly, from (1.1) - (1.3) we find

$$2Q_{m+n}(a) = (a^2 + 4)\, P_m(a)\, P_n(a) + Q_m(a)\, Q_n(a) \qquad (1.9)$$

$$Q_n(a)^2 = Q_{2n}(a) + (-1)^n.2. \qquad (1.10)$$

$$Q_n(a)^2 = (a^2 + 4)\, P_n(a)^2 + (-1)^n.4. \qquad (1.11)$$

Now from (1.11), obviously $2 \mid Q_n(a) \Leftrightarrow 2 \mid P_n(a)$. Also, from (1.2)

$$\begin{aligned} P_{3n}(a) &= \tfrac{1}{bd^2}\,(\alpha^{3n} - \beta^{3n}) \\ &= \tfrac{1}{bd^2}\,(\alpha^n - \beta^n)(\alpha^{2n} + \beta^{2n} + (-1)^n) \\ &= P_n(a)\,(Q_n(a)^2 - (-1)^n) \end{aligned}$$

Thus, since $2 \mid Q_n(a) \Leftrightarrow 2 \mid P_n(a)$, either $2 \mid P_n(a)$ or $2 \mid (Q_n(a)^2 - (-1)^n)$, i.e. $2 \mid P_{3n}(a)$. Now from (1.4)

$$P_{3n}(a) = aP_{3n-1}(a) + P_{3n-2}(a)$$

and since a is odd, therefore, $P_{3n-1}(a)$ and $P_{3n-2}(a)$ are either both odd or both even. But if they are both even, $P_n(a)$ is even for all integers n, which we have supposed not to be the case. Hence $P_{3n-1}(a)$ and $P_{3n-2}(a)$ are both odd and

$$2 \mid P_n(a) \Leftrightarrow 2 \mid Q_n(a) \Leftrightarrow 3 \mid n. \qquad (1.12)$$

(1.11) and (1.12) now give

$$(P_n(a), Q_n(a)) = 1 \text{ if } 3 \nmid n; \quad (P_n(a), Q_n(a)) = 2 \text{ if } 3 \mid n \qquad (1.13)$$

From (1.8) we find

$$\begin{aligned} 2P_{n+12}(a) &= P_n(a)Q_{12}(a) + P_{12}(a)Q_n(a) \\ &= P_n(a)(Q_6(a)^2 - 2) + Q_n(a)P_6(a)Q_6(a) \\ &\qquad \text{from (1.8) and (1.10)} \end{aligned}$$

$$= P_n(a)\left((a^2 + 4)P_6(a)^2 + 2\right) + Q_n(a)P_6(a)Q_6(a)$$

from (1.11)

$$\equiv 2P_n(a) \pmod{2P_6(a)} \text{ since } 2 \mid P_6(a),\ 2 \mid Q_6(a)$$

from (1.12).

But now $P_6(a) = a^5 + 4a^3 + 3a \equiv 0 \pmod 8$ and therefore

$$2P_{n+12}(a) \equiv 2P_n(a) \pmod{16}.$$

By similar means we may prove all the following:

$$P_{n+12}(a) \equiv P_n(a) \pmod 8 : P_{n+24}(a) \equiv P_n(a) \pmod{16} \tag{1.14}$$

$$Q_{n+12}(a) \equiv Q_n(a) \pmod 8 : Q_{n+24}(a) \equiv Q_n(a) \pmod{16} \tag{1.15}$$

Throughout this work k will denote an integer, not necessarily positive, which is even but not divisible by 3. From (1.10)

$$Q_k(a) = Q_{\frac{1}{2}k}(a)^2 - (-1)^{\frac{1}{2}k}.2$$

and thus, from (1.12), since $3 \nmid k$

$$\begin{aligned} &Q_k(a) > 0,\ Q_k(a) \equiv 3 \pmod 8 \text{ if } \tfrac{1}{2}k \text{ is odd,} \\ &\qquad Q_k(a) \equiv 7 \pmod 8 \text{ if } \tfrac{1}{2}k \text{ is even} \end{aligned} \tag{1.16}$$

Now from (1.8)

$$2P_{m+2N}(a) = P_m(a)Q_{2N}(a) + Q_m(a)P_{2N}(a)$$

$$= P_m(a)(Q_N(a)^2 - (-1)^N.2) + Q_m(a)P_N(a)Q_N(a)$$

from (1.8) and (1.10)

$$\equiv \begin{cases} (-1)^{N-1}.2P_m(a) & (\text{mod } Q_N(a)) \text{ if } 3\nmid N \\ (-1)^{N-1}.2P_m(a) & (\text{mod } 2Q_N(a)) \text{ if } 3 \mid N \end{cases}$$

from (1.12)

Thus, in either case, from (1.12)

$$P_{m+2N}(a) \equiv (-1)^{N-1} P_m(a) \quad (\text{mod } Q_N(a)) \tag{1.17}$$

Similarly we find

$$Q_{m+2N}(a) \equiv (-1)^{N-1} Q_m(a) \quad (\text{mod } Q_N(a)) \tag{1.18}$$

$$P_{m+2N}(a) \equiv (-1)^{N} P_m(a) \quad (\text{mod } P_N(a)) \tag{1.19}$$

$$Q_{m+2N}(a) \equiv (-1)^{N} Q_m(a) \quad (\text{mod}(a^2+4)P_N(a)) \tag{1.20}$$

Using (1.16) - (1.18) we find that:

$$P_{m+2k}(a) \equiv -P_m(a) \quad (\text{mod } Q_k(a)) \tag{1.21}$$

$$Q_{m+2k}(a) \equiv -Q_m(a) \quad (\text{mod } Q_k(a)) \tag{1.22}$$

Also, taking N = 1 in (1.18) and (1.20) we have, by induction:

$$Q_{2n}(a) \equiv 2 \ (\text{mod } a) \tag{1.23}$$

$$Q_{2n}(a) \equiv (-1)^n.2 \ (\text{mod } a^2+4) \tag{1.24}$$

Then, from (1.9) and (1.24)

$$Q_{2n+1}(a) \equiv (-1)^n.a \ (\text{mod } a^2+4) \tag{1.25}$$

From (1.8), clearly,

$$2P_{n+2}(a) = P_n(a)(a^2+2) + Q_n(a).a$$

$$\equiv -2P_n(a) + aQ_n(a) \quad (\text{mod } a^2+4)$$

Using this equation and (1.24) and (1.25), by an inductive

arguement we can show

$$P_{2n}(a) \equiv (-1)^{n-1}.na \pmod{a^2 + 4} \qquad (1.26)$$

$$P_{2n+1}(a) \equiv (-1)^{n}.(2n + 1) \pmod{a^2 + 4} \qquad (1.27)$$

From (1.23) and (1.16) we have

$$(a / \tilde{Q}_k(a)) = (-1 / a)(Q_k(a) / a) = (-1 / a)(2 / a) = (-2 / a)$$

i.e.

$$(Q_1(a) / Q_k(a)) = (-2 / a) \qquad (1.28)$$

Now since $2|k$, $3\nmid k$, $k \equiv \pm 2 \pmod 6$ and thus, from (1.18) and (1.7), we have

$$Q_k(a) \equiv Q_{k-6}(a) \equiv \cdots\cdots \equiv Q_{\pm 2}(a) \equiv Q_2(a) \pmod{Q_3(a)}$$

whence

$$Q_k(a) \equiv Q_2(a) \equiv a^2 + 2 \pmod{\tfrac{1}{4}(a^2 + 3)}$$

$$\equiv -1 \pmod{\tfrac{1}{4}(a^2 + 3)}$$

Thus we obtain

$$(Q_3(a) / Q_k(a)) = (4 / Q_k(a))(a / Q_k(a))(\tfrac{1}{4}(a^2 + 3) / Q_k(a))$$

$$= (a / Q_k(a))(-Q_k(a) / \tfrac{1}{4}(a^2 + 3)) \text{ by (1.16)}$$

$$= (a / Q_k(a))(1 / \tfrac{1}{4}(a^2 + 3))$$

$$= (a / Q_k(a))$$

which, with (1.28) gives

$$(Q_3(a) / Q_k(a)) = (-2 / a) \qquad (1.29)$$

By a similar arguement we find that

$$\text{if } 2\nmid n,\ 3\nmid n, \text{ then } (Q_{3n}(a) \,/\, Q_{kn}(a)) = (Q_n(a) \,/\, Q_{kn}(a)) \tag{1.30}$$

Now let n be an integer such that $2\nmid n$, $3\nmid n$, and suppose that $Q_n(a)^2 + 1 = 2y^2$. Then, since n is odd, from (1.10) we have

$$Q_{2n}(a) = 2y^2 + 1.$$

Suppose first that $n \equiv 1 \pmod 4$. Then if $n \neq 1$, let $n = 1 + rk$ where r is odd and $k = 2^m$, $m > 1$. Then

$$\begin{aligned} 2y^2 + 1 = Q_{2n}(a) &= Q_{2 + 2rk}(a) \\ &\equiv (-1)^r Q_2(a) \pmod{Q_k(a)} \end{aligned}$$

by repeated applications of (1.22). Thus, since r is odd,

$$2y^2 + 1 \equiv -(a^2 + 2) \pmod{Q_k(a)}$$

i.e.

$$4y^2 \equiv -2(a^2 + 3) \pmod{Q_k(a)}$$

Hence, since $a(a^2 + 3) = Q_3(a)$ and $(Q_3(a), Q_k(a)) = 1$,

$$\begin{aligned} 1 &= (-2 \,/\, Q_k(a))\ (a^2 + 3 \,/\, Q_k(a)) \\ &= -(a^2 \,/\, Q_k(a))\ (a^2 + 3 \,/\, Q_k(a)) \text{ by (1.16) since } 4\mid k \\ &= -(a \,/\, Q_k(a))\ (a(a^2 + 3) \,/\, Q_k(a)) \\ &= -(a \,/\, Q_k(a))^2 \text{ by (1.30) with } n = 1 \\ &= -1. \end{aligned}$$

This is clearly impossible. Thus if $Q_n(a)^2 + 1 = 2y^2$ and $n \equiv 1 \pmod 4$ then $n = 1$.

If $n \equiv 3 \pmod 4$, we have $Q_{2n}(a) = 2y^2 + 1 = Q_{-2n}(a)$ by (1.7) where $-n \equiv 1 \pmod 4$ and this is therefore only possible for $-n = 1$. Hence we have

$$\text{if } 2\nmid n,\ 3\nmid n, \text{ then if } Q_n(a)^2 + 1 = 2y^2, n = \pm 1 \qquad (1.31)$$

Now from (1.2) and (1.3)

$$\alpha^{2n+1} = \tfrac{1}{2}\left(Q_{2n+1}(a) + bd^{\frac{1}{2}}P_{2n+1}(a)\right)$$

$$\beta^{2n+1} = \tfrac{1}{2}\left(Q_{2n+1}(a) - bd^{\frac{1}{2}}P_{2n+1}(a)\right)$$

and hence

$$P_m\left(Q_{2n+1}(a)\right) = \frac{1}{bP_{2n+1}(a)d^{\frac{1}{2}}}\left(\alpha^{m(2n+1)} - \beta^{m(2n+1)}\right)$$

$$= \frac{P_{m(2n+1)}(a)}{P_{2n+1}(a)}$$

i.e.

$$P_{m(2n+1)}(a) = P_{2n+1}(a)\ P_m\left(Q_{2n+1}(a)\right) \qquad (1.32)$$

Similarly we find

$$Q_{m(2n+1)}(a) = Q_m\left(Q_{2n+1}(a)\right) \qquad (1.33)$$

Finally we observe that if $2\alpha = a + bd^{\frac{1}{2}}$ is the fundamental solution of the equation $X^2 - dY^2 = -4$, and a and b are both odd, then the fundamental solutions of the equations $X^2 - dY^2 = 4$, $X^2 - dY^2 = -1$ and $X^2 - dY^2 = 1$ are respectively $2\alpha^2$, α^3, and α^6. Hence

the general solution of $X^2 - dY^2 = -4$ is $X = Q_{2n-1}(a), Y = bP_{2n-1}(a)$

(I.I)

the general solution of $X^2 - dY^2 = 4$ is $X = Q_{2n}(a)$, $Y = bP_{2n}(a)$ (I.II)

the general solution of $X^2 - dY^2 = -1$ is $X = \frac{1}{2}Q_{6n-3}(a)$, $Y = \frac{1}{2}bP_{6n-3}(a)$ (I.III)

the general solution of $X^2 - dY^2 = 1$ is $X = \frac{1}{2}Q_{6n}(a)$, $Y = \frac{1}{2}bP_{6n}(a)$ (I.IV).

We are seeking solutions of the equations $X^2 - dY^4 = \pm 1, \pm 4$; $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dN^2Y^4 = \pm 1, \pm 4$ and $N^2X^4 - dY^2 = \pm 1, \pm 4$. Clearly the solutions of $X^4 - dY^2 = -4$ are given by $X^2 = Q_{2n-1}(a)$, $Y = bP_{2n-1}(a)$ and those of $X^2 - dN^2Y^4 = 1$ by $X = \frac{1}{2}Q_{6n}(a)$, $NY^2 = \frac{1}{2}bP_{6n}(a)$ with similar results for the other equations. We therefore wish to prove theorems which will enable us to say when $P_n(a) = Y^2, NY^2$; $Q_n(a) = X^2, NX^2$ where N is a square-free integer. We are already in a position to deal with the cases $Q_n(a) = X^2, 2X^2$; $P_n(a) = Y^2, 2Y^2$. The results are contained in the following four theorems.

THEOREM 1.1. The equation $Q_n(a) = X^2$ has

(a) two solutions $n = 1,3$ if $a = 1$;

(b) one solution $n = 3$ if $a = 3$;

(c) one solution $n = 1$ if a is a perfect square, $a \neq 1$;

(d) no solutions otherwise.

Proof. (i) If n is even, by (1.10) we have

$$Q_n(a) = Q_{\frac{1}{2}n}(a)^2 \pm 2 \neq X^2.$$

(ii) If $a \equiv 5$ or $7 \pmod 8$ and n is odd, then $Q_n(a) \neq X^2$. For $Q_{-1}(a) = -a \neq X^2$, $Q_{-3}(a) = -a(a^2 + 3) \neq X^2$, whereas if $n \neq -1$ or -3 we can choose $r \geq 0$ and k such that $n = -t + 2.3^r.k$ where $2|k$, $3\nmid k$, and $t = 1$ or 3. Then repeated applications of (1.22) give

$$Q_n(a) = Q_{-t + 2.3^r.k}(a) \equiv (-1)^{3r} Q_{-t}(a) \pmod{Q_k(a)}$$

$$\equiv Q_t(a) \pmod{Q_k(a)} \text{ by (1.7).}$$

Since $2|k$, $3\nmid k$, $(Q_t(a), Q_k(a)) = 1$ and hence

$$(Q_n(a) / Q_k(a)) = (Q_t(a) / Q_k(a)) = (-2 / a) \text{ from (1.28) and (1.29)}$$

$$= -1$$

since $a \equiv 5$ or $7 \pmod 8$. Thus $Q_n(a) \neq X^2$.

(iii) If $a \equiv 1$ or $3 \pmod 8$ and n is odd, then $Q_n(a) \neq X^2$, except possibly for $n = 1$ or 3. For if $n \neq 1$ or 3 we can choose as before $r \geqslant 0$ and k such that $n = t + 2.3^r.k$ where $2|k$, $3\nmid k$, and $t = 1$ or 3. Repeated applications of (1.22) then give

$$Q_n(a) \equiv (-1)^{3r} Q_t(a) \pmod{Q_k(a)}$$

$$\equiv -Q_t(a) \pmod{Q_k(a)} \text{ by (1.7)}$$

Thus again, since $(Q_t(a), Q_k(a)) = 1$,

$$(Q_n(a) / Q_k(a)) = (-Q_t(a) / Q_k(a)) = -(-2 / a) \text{ from (1.16) (1.28) and (1.29)}$$

$$= -1$$

since $a \equiv 1$ or $3 \pmod 8$.

(iv) If $n = 1$, $Q_n(a) = a = X^2$ if and only if a is a perfect square. If $n = 3$, $Q_n(a) = a(a^2 + 3)$ where it is obvious that $(a, a^2 + 3) = 1$ or 3. Thus, if $Q_n(a) = X^2$, we require either

$$a = X_1^2, \quad a^2 + 3 = X_2^2$$

which is clearly only possible for $a = 1$, or

$$a = 3X_1^2, \quad a^2 + 3 = 3X_2^2$$

whence

$$X_2^2 - 3X_1^4 = 1.$$

But now, by (7), this equation has only the solutions $X_1 = 0, \pm 1, \pm 2$ and so, since a is odd, $a = 3$ is the only possibility.

This completes the proof of the theorem.

THEOREM 1.2. The equation $Q_n(a) = 2X^2$ has

(a) three solutions $n = 0, \pm 6$ if $a = 1$ or 5;

(b) one solution $n = 0$ otherwise.

Proof. (i) If n is odd, $Q_n(a) \neq 2X^2$. For, by (1.12), if $Q_n(a)$ is even $3|n$, and if in addition n is odd we have $n \equiv \pm 3 \pmod{12}$. Then by (1.7) and (1.15)

$$Q_n(a) \equiv Q_{\pm 3}(a) \equiv Q_3(a) \equiv 4 \pmod 8$$

whence $Q_n(a) \neq 2X^2$.

(ii) If $n \equiv 0 \pmod 4$, then $Q_n(a) = 2X^2$ only for $n = 0$. For $Q_0(a) = 2$, whereas if $n \neq 0$ we may write $n = 2.3^r k$ for some $r \geqslant 0$ and k where $2|k$, $3\nmid k$. Then by (1.22)

$$Q_n(a) \equiv -Q_0(a) \equiv -2 \pmod{Q_k(a)}$$

and hence

$$(2Q_n(a) / Q_k(a)) = (-4 / Q_k(a)) = -1 \text{ by (1.16)}$$

Thus $Q_n(a) \neq 2X^2$.

(iii) If $n \equiv 6 \pmod 8$, then $Q_n(a) \neq 2X^2$ except possibly for $n = 6$. For if $n \neq 6$ we may write $n = 6 + 2.3^r.k$ where now $4|k$, $3\nmid k$. Then as before

$$Q_n(a) \equiv -Q_6(a) \pmod{Q_k(a)}$$

Now by (1.18)

$$2Q_k(a) \equiv -2Q_{k-12}(a) \equiv \cdots\cdots \equiv \pm 2Q_{\pm 4}(a) \pmod{Q_6(a)}$$

since $4|k$, $3\nmid k$.

$Q_2(a) \equiv 3 \pmod 8$, $Q_4(a) \equiv 7 \pmod 8$ and $\frac{1}{2}Q_6(a) \equiv 1 \pmod 4$

Thus we have

$$\begin{aligned}(2Q_n(a) \,/\, Q_k(a)) &= (-2Q_6(a) \,/\, Q_k(a)) = -(\tfrac{1}{2}Q_6(a) \,/\, Q_k(a)) \\ &\qquad\qquad \text{by (1.16)} \\ &= -(Q_k(a) \,/\, \tfrac{1}{2}Q_6(a)) = -(\pm Q_4(a) \,/\, \tfrac{1}{2}Q_6(a)) \\ &= -(Q_4(a) \,/\, \tfrac{1}{2}Q_6(a)) = -(\tfrac{1}{2}Q_6(a) \,/\, Q_4(a)) \\ &= -(Q_6(a) \,/\, Q_4(a)) = -(-Q_{-2}(a) \,/\, Q_4(a)) \\ &\qquad\qquad \text{by (1.22)} \\ &= (Q_2(a) \,/\, Q_4(a)) \text{ by (1.7) and (1.16)} \\ &= -(Q_4(a) \,/\, Q_2(a)) = -(-2 \,/\, Q_2(a)) \text{ by (1.10)} \\ &= -1.\end{aligned}$$

Thus again $Q_n(a) \neq 2X^2$.

(iv) If $n \equiv 2 \pmod 8$, $Q_n(a) \neq 2X^2$ except possibly for $n = -6$.

For by (1.7) if n is even $Q_{-n}(a) = Q_n(a)$ and if $n \equiv 2 \pmod 8$ $-n \equiv 6 \pmod 8$ and the result follows from the previous one.

(v) If

$$\begin{aligned}2X^2 = Q_{\pm 6}(a) &= a^6 + 6a^4 + 9a^2 + 2 \\ &= (a^2 + 2)(a^4 + 4a^2 + 1) \\ &= c(c^2 - 3)\end{aligned}$$

where $c = a^2 + 2 \equiv 3 \pmod 8$, then either

$$c = X_1^2 \;;\; c^2 - 3 = 2X_2^2$$

which is impossible since $c \equiv 3 \pmod 8$, or

$$c = 3X_1^2 \; ; \; c^2 - 3 = 6X_2^2$$

whence

$$2X_2^2 = 3X_1^4 - 1.$$

But now R.T.Bumby has shown, in (1), that this equation has only the solutions $X_1 = 1$ or 3, i.e. $Q_{\pm 6}(a) = 2X^2$ only for $a = 1$ or 5.

This completes the proof of the theorem.

THEOREM 1.3. The equation $P_n(a) = Y^2$ has

(a) five solutions $n = 0, \pm 1, 2, 12$ if $a = 1$;

(b) four solutions $n = 0, \pm 1, 2$ if a is a perfect square, $a \neq 1$;

(c) three solutions $n = 0, \pm 1$ otherwise.

Proof. (i) If n is even and $P_n(a) = Y^2$ we have, by (1.8),

$$Y^2 = P_{\frac{1}{2}n}(a) \; Q_{\frac{1}{2}n}(a).$$

Thus from (1.13) we must have either

$$3 \nmid n \quad P_{\frac{1}{2}n}(a) = Y_1^2 \; ; \; Q_{\frac{1}{2}n}(a) = Y_2^2$$

and by theorem 1.1 this is possible only for $\frac{1}{2}n = 1$ and a a perfect square, or

$$3 \mid n \quad P_{\frac{1}{2}n}(a) = 2Y_1^2 \; \& \; Q_{\frac{1}{2}n}(a) = 2Y_2^2$$

Now by theorem 1.2 the latter is possible for $\frac{1}{2}n = 0, \pm 6$. Of these values, 0 always satisfies $P_{\frac{1}{2}n}(a) = 2Y_1^2$ and -6 never since $P_{-6}(a)$ is negative by (1.6). The remaining possibility, $\frac{1}{2}n = 6$ requires

$$2Y_1^2 = P_6(a) = P_3(a) \; Q_3(a) \quad \text{by (1.8)}$$

Thus, by (1.13) we require either

$$P_3(a) = Y_3^2 \; ; \; Q_3(a) = 2Y_4^2$$

which from theorem 1.2 is impossible, or

$$P_3(a) = 2Y_3^2 \; ; \; Q_3(a) = Y_4^2$$

By theorem 1.1 the latter is possible only for a = 1 or 3.
$P_3(1) = 2$, which satisfies $P_3(a) = 2Y_3^2$, whereas $P_3(3) = 10$, which does not.

(ii) If n is odd, $P_n(a) \neq Y^2$ except for $n = \pm 1$. For $P_{\pm 1}(a) = 1$ whereas if $n \neq \pm 1$, we write $n = \pm 1 + 2,3^r.k$ as before. Then repeated applications of (1.21) give

$$P_n(a) \equiv -P_{\pm 1}(a) \equiv -P_1(a) \pmod{Q_k(a)} \text{ by (1.6)}$$
$$\equiv -1$$

Thus

$$(P_n(a) \,/\, Q_k(a)) = (-1 \,/\, Q_k(a)) = -1 \text{ by (1.16).}$$

Hence $P_n(a) = Y^2$ only for $n = \pm 1$.
This completes the proof of the theorem.

THEOREM 1.4. The equation $P_n(a) = 2Y^2$ has

(a) two solutions n = 0,6 if a = 1;

(b) three solutions n = 0, ± 3 if $a = \frac{1}{2}Q_{2n+1}(2)$;

(c) one solution n = 0 otherwise.

Proof. We note first that, from (1.13), if $P_n(a) = 2Y^2$ then $3 \mid n$.

(i) If n is even, from (1.8) we have

$$P_n(a) = P_{\frac{1}{2}n}(a)\, Q_{\frac{1}{2}n}(a)$$

and so since $3 \mid n$ from (1.13) we see that if $P_n(a) = 2Y^2$ we must have either

$$P_{\frac{1}{2}n}(a) = 2Y_1^2 \; ; \; Q_{\frac{1}{2}n}(a) = Y_2^2$$

and from theorem 1.1 since $3|n$ the latter equation is satisfied only by $\frac{1}{2}n = 3$, $a = 1$ or 3 where as before only $a = 1$ gives a solution of the first equation, or

$$P_{\frac{1}{2}n}(a) = Y_1^2 \; ; \; Q_{\frac{1}{2}n}(a) = 2Y_2^2$$

By theorem 1.3 the first of these is satisfied only by $\frac{1}{2}n = 0$ and, if $a = 1$, $\frac{1}{2}n = 12$. By theorem 1.2 $\frac{1}{2}n = 0$ satisfies the second equation whereas $\frac{1}{2}n = 12$ does not.

(ii) If n is odd from our first remark we may write $n = 3m$ where m is odd. Then from (1.8) and (1.9) we find

$$P_{3m}(a) = P_m(a)\left((a^2 + 4)\,P_m(a)^2 - 3\right)$$

and clearly $(P_m(a),\ (a^2 + 4)\,P_m(a)^2 - 3) = 1$ or 3. But since m is odd from (1.11)

$$Q_m(a)^2 - (a^2 + 4)\,P_m(a)^2 = -4$$

and so $3 \nmid P_m(a)$. Thus if $P_{3m}(a) = 2Y^2$ we must have either

$$P_m(a) = 2Y_1^2 \; ; \; (a^2 + 4)\,P_m(a)^2 - 3 = Y_2^2$$

and by (1.11) this requires $Q_m(a)^2 + 1 = Y_2^2$ which is impossible, or

$$P_m(a) = Y_1^2 \; ; \; (a^2 + 4)\,P_m(a)^2 - 3 = 2Y_2^2$$

Since m is odd from theorem 1.3 the only possibilities are $m = \pm 1$, i.e. $n = \pm 3$. But from (1.11) we then require $Q_{\pm 1}(a)^2 + 1 = 2Y_2^2$ or

$$\left(2Q_{\pm 1}(a)\right)^2 - (2^2 + 4)\,Y_2^2 = -4$$

i.e. $2a = Q_{2n+1}(2)$.

This concludes the proof of the theorem.

We are seeking solutions of the equations $P_n(a) = Y^2, NY^2$; $Q_n(a) = X^2, NX^2$ where N is a square-free integer and have now dealt with the cases $P_n(a) = Y^2, 2Y^2$; $Q_n(a) = X^2, 2X^2$ in theorems 1.1 - 1.4. It turns out to be most profitable next to drop the restriction that N must be square-free and consider $N = P_m(a), 2P_m(a), Q_m(a)$ and $2Q_m(a)$. Before we can proceed to the solution of the equations $P_n(a) = NY^2$; $Q_n(a) = NX^2$ for these values of N, however, we must establish for what values of n $P_m(a) \mid P_n(a)$ with corresponding results for the other functions. The results are contained in the following six lemmas.

LEMMA 1.1. $P_m(a) \mid P_{rm}(a)$ for any integer r.

Proof. From (1.6) we need only consider $r \geq 0$. Hence we use proof by induction. The result is obviously true for $r = 0,1$. Now from (1.1), (1.2) and (1.3)

$$\begin{aligned} P_{(r+2)m}(a) &= \frac{1}{bd^{\frac{1}{2}}}(\alpha^{(r+2)m} - \beta^{(r+2)m}) \\ &= \frac{1}{bd^{\frac{1}{2}}}(\alpha^m + \beta^m)(\alpha^{(r+1)m} - \beta^{(r+1)m}) \\ &\quad - (\tfrac{\alpha\beta}{bd^2})^m(\alpha^{rm} - \beta^{rm}) \\ &= Q_m(a)\, P_{(r+1)m}(a) + (-1)^{m-1} P_{rm}(a) \end{aligned}$$

Thus if we assume $P_m(a) \mid P_{tm}(a)$ for all $t \leq r + 1$, $r \geq 0$, then $P_m(a) \mid P_{(r+2)m}(a)$. Hence the result by induction.

LEMMA 1.2. $Q_m(a) \mid Q_{rm}(a)$ for any odd integer r.

Proof. From (1.7) again we need only consider $r \geq 0$ and so we use proof by induction. The result is obviously true for $r = 1$. Now from (1.1), (1.2) and (1.3)

$$Q_{(r+2)m}(a) = \alpha^{(r+2)m} + \beta^{(r+2)m} = (\alpha^{(r+1)m} + \beta^{(r+1)m}) \times$$

$$(\alpha^{m} + \beta^{m}) - (\alpha\beta)^{m}(\alpha^{rm} + \beta^{rm})$$

$$= Q_m(a)\, Q_{(r+1)m}(a) + (-1)^{m-1} Q_{rm}(a)$$

Thus if we assume the result true for all odd integers $t \leq r$, it is clearly true for $r + 2$. Hence the result by induction.

LEMMA 1.3. $(Q_{rm}(a), Q_m(a)) \mid 2$ for every even integer r.

Proof. As in the proof of lemma 1.2

$$Q_{(r+2)m}(a) = Q_m(a)\, Q_{(r+1)m}(a) + (-1)^{m-1} Q_{rm}(a)$$

for all integers r. Thus if r is even repeated applications of the above result show that

$$Q_{(r+2)m}(a) \equiv \pm Q_o(a) \pmod{Q_m(a)}$$

$$\equiv \pm 2 \pmod{Q_m(a)}$$

Hence the result.

LEMMA 1.4. $(P_m(a), P_n(a)) = P_{(m,n)}(a)$.

Proof. Let $(m,n) = r$. Then it is a well known fact that there exist integers g and h such that $gn + hm = r$. Thus, from (1.8) we find

$$2P_r(a) = P_{gn}(a)\, Q_{hm}(a) + P_{hm}(a)\, Q_{gn}(a) \qquad (*)$$

From lemma 1.1 $P_n(a) \mid P_{gn}(a)$ and $P_m(a) \mid P_{hm}(a)$. Thus $(P_n(a), P_m(a)) \mid 2P_r(a)$. Also, from lemma 1.1, $P_r(a) \mid P_n(a)$ and $P_r(a) \mid P_m(a)$ and therefore $(P_m(a), P_n(a)) = P_r(a)$ or $2P_r(a)$. Obviously if either $P_m(a)$ or $P_n(a)$ is odd $(P_m(a), P_n(a)) = P_r(a)$.

If they are both even from lemma 1.1 clearly $P_{gn}(a)$ and $P_{hm}(a)$ are both even. Then from (1.12) we see that $Q_{gn}(a)$ and $Q_{hm}(a)$ are both even. Thus from (*) we may obtain

$$P_r(a) = P_{gn}(a)\left(\tfrac{1}{2}Q_{hm}(a)\right) + P_{hm}(a)\left(\tfrac{1}{2}Q_{gn}(a)\right)$$

where $\frac{1}{2}Q_{hm}(a)$ and $\frac{1}{2}Q_{gn}(a)$ are integers. Then as above
$(P_m(a), P_n(a)) = P_r(a)$
This completes the proof.

LEMMA 1.5. Let $(m,n) = r$ and let $\frac{n}{r}$ be odd. Then

(a) if $\frac{m}{r}$ is odd $(Q_m(a), Q_n(a)) = Q_r(a)$;

(b) if $\frac{m}{r}$ is even $(Q_m(a), Q_n(a)) \mid 2$.

Proof. Since $(m,n) = r$ there exist g and h such that $gn + hm = r$. Then (1.9) gives

$$2Q_r(a) = (a^2 + 4)P_{gn}(a)P_{hm}(a) + Q_{gn}(a)Q_{hm}(a) \qquad (**)$$

(a). If $\frac{m}{r}$ and $\frac{n}{r}$ are both odd, g and h will be of opposite parity. We may assume without loss of generality that h is odd. Then by lemma 1.2 $Q_m(a) \mid Q_{hm}(a)$. Since g is even, by lemma 1.1 $P_{2n}(a) \mid P_{gn}(a)$; but from (1.8) $P_{2n}(a) = P_n(a)Q_n(a)$ and thus $Q_n(a) \mid P_{gn}(a)$. Hence $(Q_m(a), Q_n(a)) \mid 2Q_r(a)$. Since $\frac{m}{r}$ and $\frac{n}{r}$ are both odd, from lemma 1.2 $Q_r(a) \mid Q_m(a)$ and $Q_r(a) \mid Q_n(a)$ and so $(Q_m(a), Q_n(a)) = Q_r(a)$ or $2Q_r(a)$. By a method similar to that used at the end of the proof of lemma 1.4 we may show that $(Q_m(a), Q_n(a)) = 2Q_r(a)$ is impossible.

(b) If $\frac{m}{r}$ is even, g must be odd.

(i) If h is even as above we can show that $(Q_m(a), Q_n(a)) \mid 2Q_r(a)$. Also, since $\frac{n}{r}$ is odd $Q_r(a) \mid Q_n(a)$ by lemma 1.2. But since $\frac{m}{r}$ is

even, as in the proof of lemma 1.3, $Q_m(a) \equiv \pm 2 \pmod{Q_r(a)}$ and thus $(Q_m(a), Q_n(a)) \mid 4$. But now m is even and therefore, from (1.10), $Q_m(a) = Q_{\frac{1}{2}m}(a)^2 \pm 2$ and hence $Q_m(a)$ is either odd or congruent to 2 (mod 8). Therefore $(Q_m(a), Q_n(a)) \mid 2$.

(ii) If h is odd as before we have

$$2P_r(a) = P_{gn}(a)\, Q_{hm}(a) + P_{hm}(a)\, Q_{gn}(a) \qquad (*)$$

where $Q_m(a) \mid Q_{hm}(a)$ and $Q_n(a) \mid Q_{gn}(a)$ from lemma 1.2. Thus $(Q_m(a), Q_n(a)) \mid 2P_r(a)$. Since m is even, however, from (1.10) and (1.11) $Q_m(a) = Q_{\frac{1}{2}m}(a)^2 \pm 2 = (a^2 + 4)P_{\frac{1}{2}m}(a)^2 \mp 2$. Now $r \mid \frac{1}{2}m$ and thus, by lemma 1.1, $P_r(a) \mid P_{\frac{1}{2}m}(a)$. Hence $(Q_m(a), Q_n(a)) \mid 4$ and as in (i) $(Q_m(a), Q_n(a)) = 4$ is impossible.

This completes the proof.

LEMMA 1.6. Let $(m,n) = r$. Then

(a) if $\frac{m}{r}$ is odd $(P_m(a), Q_n(a)) \mid 4$;

(b) if $\frac{m}{r}$ is even $(P_m(a), Q_n(a)) = Q_r(a)$.

Proof. As before there exist g and h such that $gn + hm = r$ and

$$2P_r(a) = P_{gn}(a)Q_{hm}(a) + P_{hm}(a)Q_{gn}(a) \qquad (*)$$

$$2Q_r(a) = (a^2 + 4)P_{gn}(a)P_{hm}(a) + Q_{gn}(a)Q_{hm}(a) \qquad (**)$$

(a). (i). If $\frac{m}{r}$ is odd and g is odd then from (**) $(P_m(a), Q_n(a)) \mid 2Q_r(a)$ since $P_m(a) \mid P_{hm}(a)$ from lemma 1.1 and $Q_n(a) \mid Q_{gn}(a)$ from lemma 1.2. But since $\frac{m}{r}$ is odd, from lemma 1.2 $Q_r(a) \mid Q_m(a)$ and from (1.11) it is easily seen that $(P_m(a), Q_m(a)) \mid 2$. Therefore $(P_m(a), Q_r(a)) \mid 2$ and $(P_m(a), Q_n(a)) \mid 4$.

(ii) If $\frac{m}{r}$ is odd and g is even from (*) $(P_m(a), Q_n(a)) \mid 2P_r(a)$,

for from lemma 1.1 and (1.8) $P_m(a) \mid P_{hm}(a)$ and $P_{2n}(a)$ $= P_n(a)\, Q_n(a) \mid P_{gn}(a)$. But also from lemma 1.1, $P_r(a) \mid P_m(a)$ and from (1.11) $(P_n(a), Q_n(a)) \mid 2$. Thus again $(P_m(a), Q_n(a)) \mid 4$.

(b). If $\frac{m}{r}$ is even then g must be odd. From (**) as in (a)(i) $(P_m(a), Q_n(a)) \mid 2Q_r(a)$. From the definition of r, since $\frac{m}{r}$ is even, $\frac{n}{r}$ is odd and so from lemma 1.2 $Q_r(a) \mid Q_n(a)$. Also, since $\frac{m}{r}$ is even from lemma 1.1 and (1.8), $P_{2r}(a) = P_r(a)\, Q_r(a) \mid P_m(a)$ and so $(P_m(a), Q_n(a)) = Q_r(a)$ or $2Q_r(a)$. An arguement similar to that at the end of the proof of lemma 1.4 shows that $(P_m(a), Q_n(a)) = 2Q_r(a)$ is impossible.
This completes the proof.

COROLLARY 1.1. (of lemmas 1.4 - 1.6).

(a) If $P_m(a) \mid P_n(a)$ and $\lvert P_m(a) \rvert > 1$ then $m \mid n$;

(b) If $Q_m(a) \mid Q_n(a)$ and $\lvert Q_m(a) \rvert > 2$ then $\frac{n}{m}$ is an odd integer;

(c) If $Q_m(a) \mid P_n(a)$ and $\lvert Q_m(a) \rvert > 2$ then $\frac{n}{m}$ is an even integer;

(d) If $P_m(a) \mid Q_n(a)$ and $\lvert P_m(a) \rvert > 2$ then $m = 2$ if $a > 2$ and $m = 4$ if $a = 1$.

Proof. These results follow immediately from lemmas 1.4 - 1.6.

We are now in a position to solve the equations $P_n(a) = P_m(a)Y^2$, $2P_m(a)Y^2$, $Q_m(a)Y^2$ and $2Q_m(a)Y^2$; $Q_n(a) = Q_m(a)X^2$, $2Q_m(a)X^2$, $P_m(a)X^2$ and $2P_m(a)X^2$. The results are contained in theorems 1.5 - 1.12.

THEOREM 1.5. For any given m such that $\lvert Q_m(a) \rvert > 2$, $Q_n(a)$ is of the form $Q_m(a)\, X^2$ only for $n = m$ if m is odd and $n = \pm m$ if m is even.

Proof. We note first that since $Q_n(a) = Q_m(a)X^2$ only if $Q_m(a) \mid Q_n(a)$, from corollary 1.1 we require $n = mt$ where t is an odd integer.

(i) Suppose that $t \equiv 1 \pmod 4$. If $t = 1$, $Q_n(a) = Q_m(a)$

$= Q_m(a).1^2$, whereas if $t \neq 1$, we may write $n = m + 2.3^r.k$ where $2|k$, $3\nmid k$. Repeated applications of (1.22) then give

$$Q_n(a) \equiv (-1)^{3^r} Q_m(a) \pmod{Q_k(a)}$$

Now if 2^s is the highest power of 2 which divides m, $2^{s+1}|k$. Also $3\nmid k$. Hence from lemma 1.5 and (1.12) $(Q_m(a), Q_k(a)) = 1$ and so

$$(Q_m(a)Q_n(a) / Q_k(a)) = (-Q_m(a)^2 / Q_k(a)) = -1 \text{ by (1.16).}$$

Hence $Q_n(a) \neq Q_m(a)X^2$.

(ii) Suppose that $t \equiv 3 \pmod 4$ and m is even. Then by (1.7) $Q_n(a) = Q_{-n}(a)$ where $-n = mt'$ and $t' \equiv 1 \pmod 4$. Thus from (i) $Q_n(a) = Q_m(a)X^2$ if and only if $-n = m$ i.e. $n = -m$.

(iii) Suppose that $t \equiv 3 \pmod 4$, m is odd and $3\nmid m$. Then if $t = 3$, $Q_n(a) = Q_m(a)(Q_m(a)^2 + 3)$ from (1.8) and (1.9) and $Q_n(a) = Q_m(a)X^2$ if and only if $Q_m(a)^2 + 3 = X^2$ which is impossible since $|Q_m(a)| > 2$. If $t \neq 3$ we may write $n = 3m + 2.3^r.mk$ where $2|mk$ and $3\nmid mk$. Then as in (i) $(Q_{3m}(a), Q_{mk}(a)) = 1$ and

$$Q_n(a) \equiv (-1)^{3^r} Q_{3m}(a) \pmod{Q_{km}(a)}$$

whence

$$\begin{aligned}(Q_m(a)Q_n(a) / Q_{km}(a)) &= (-Q_m(a)Q_{3m}(a) / Q_{km}(a)) \\ &= (-Q_m(a)^2 / Q_{km}(a)) \text{ by (1.30)} \\ &= -1 \text{ by (1.16).}\end{aligned}$$

Hence $Q_n(a) \neq Q_m(a)X^2$.

(iv) Suppose finally that $t \equiv -1 \pmod 4$, m is odd and $3|m$. Then $m \equiv \pm 3 \pmod{12}$ and $n = mt \equiv \mp 3 \pmod{12}$. Now from (1.15), looking at the first 24 values of $Q_r(a)$ we see that $4|Q_m(a)$, $8\nmid Q_m(a)$ and $4|Q_n(a)$, $8\nmid Q_n(a)$ and also

$$\tfrac{1}{4}Q_m(a) \equiv -\tfrac{1}{4}Q_n(a) \pmod 4.$$

Thus if $Q_n(a) = Q_m(a)X^2$, $X^2 \equiv -1 \pmod 4$ which is impossible. This completes the proof.

THEOREM 1.6. For any given m such that $|Q_m(a)| > 2$, $Q_n(a)$ is never of the form $2Q_m(a)X^2$.

Proof. We note first that from corollary 1.1 again we require $n = mt$ where t is an odd integer.

(i) Suppose that m is even. Then if $t = \pm 1$, $Q_n(a) = Q_{\pm m}(a) \neq 2Q_m(a)X^2$, whereas if $t \neq \pm 1$, since m is even we may write $n = \pm m + 2.3^r.k$ where $4|k$, $3\nmid k$. Then by repeated applications of (1.22)

$$Q_n(a) \equiv (-1)^{3^r} Q_{\pm m}(a) \pmod{Q_k(a)}$$
$$\equiv -Q_m(a) \text{ by (1.7) since m is even.}$$

If 2^s is the highest power of 2 which divides m, $2^{s+1}|k$ and so from lemma 1.5 and (1.12) $(Q_m(a), Q_k(a)) = 1$. Hence

$$(2Q_m(a)\, Q_n(a) / Q_k(a)) = (-2Q_m(a)^2 / Q_k(a))$$
$$= -1 \text{ by (1.16) since } 4|k.$$

Thus $Q_n(a) \neq 2Q_m(a)X^2$.

(ii) Suppose now that m is odd. Then n is odd. Also, since we require $Q_n(a)$ to be even, $3|n$, from (1.12). Then (1.15) together with the first 12 values of $Q_n(a)$ shows that $Q_n(a) \equiv 4 \pmod 8$.

But also, since m is odd, (1.15) and the first 12 values of $Q_m(a)$ show that $Q_m(a)$ is either odd or congruent to 4 (mod 8). Hence it is impossible that $Q_n(a) = 2Q_m(a)X^2$.

This completes the proof.

THEOREM 1.7. For any given m such that $|P_m(a)| > 2$, $P_n(a)$ is

of the form $P_m(a)Y^2$ only for $n = 0$, $n = m$ if m is even, $n = \pm m$ if m is odd and ($a = 3$, $m = \pm 3$, $n = 6$).

Proof. We note first that from corollary 1.1 if $P_n(a) = P_m(a)Y^2$ then $n = mt$ for some integer t.

(i) Suppose first that t is even. Put $t = 2t'$. Then from (1.8)

$$P_n(a) = P_{mt'}(a)\, Q_{mt'}(a)$$

and by (1.13) $(P_{mt'}(a), Q_{mt'}(a)) = 1$ or 2. Also by lemma 1.1 $P_m(a) \mid P_{mt'}(a)$ and thus if $P_n(a) = P_m(a)Y^2$ we need either

$$P_{mt'}(a) = P_m(a)Y_1^2 \; ; \; Q_{mt'}(a) = Y_2^2$$

where from theorem 1.1 the only possible solution is $Q_3(3) = Y_2^2$, or

$$P_{mt'}(a) = 2P_m(a)Y_1^2 \; ; \; Q_{mt'}(a) = 2Y_2^2$$

From theorem 1.2 the only possible solutions here are $Q_o(a) = 2$, $Q_{\pm 6}(1) = 2Y_2^2$, $Q_{\pm 6}(5) = 2Y_2^2$.

These possibilities lead only to the solutions $n = 0$ and ($a = 3$, $m = \pm 3$, $n = 6$) since the equations $P_{\pm 6}(a) = 2P_m(a)Y_1^2$ have no solutions for $a = 1$ or 5.

(ii) Suppose now that t is odd but m is even. Put $m = 2m'$ and as before we have

$$P_n(a) = P_{m't}(a)\, Q_{m't}(a)$$

where $(P_{m't}(a), Q_{m't}(a) = 1$ or 2. Since t is odd, by lemmas 1.1 and 1.2 $P_{m'}(a) \mid P_m(a)$ and $Q_{m'}(a) \mid Q_m(a)$. Also, from (1.8), $P_m(a) = P_{m'}(a)\, Q_{m'}(a)$ and so, if $P_n(a) = P_m(a)Y^2$, either

$$P_{m't}(a) = 2P_{m'}(a)Y_1^2 \; ; \; Q_{m't}(a) = 2Q_{m'}(a)Y_2^2$$

where, from theorem 1.6 the second equation has no solutions, or

$$P_{m',t}(a) = P_{m'}(a)Y_1^2 \; ; \quad Q_{m',t}(a) = Q_{m'}(a)Y_2^2$$

where, from theorem 1.5, the second equation requires $t = \pm 1$. Since m is even $P_{-m}(a) = -P_m(a)$ and so the only solution is $t = 1$.

(iii) Suppose finally that t and m are both odd. If $t = \pm 1$, $P_n(a) = P_m(a) = P_m(a).1^2$, whereas if $t \neq \pm 1$, we may write as usual $n = \pm m + 2.3^r.k$. Repeated applications of (1.21) then give

$$P_n(a) \equiv (-1)^{3^r} P_{\pm m}(a) \pmod{Q_k(a)}$$

$$\equiv -P_m(a) \pmod{Q_k(a)} \text{ by (1.6)}$$

Since m is odd and $3 \nmid k$, by lemma 1.6 and (1.12) $(P_m(a), Q_k(a)) = 1$. Thus

$$(P_m(a)\, P_n(a) / Q_k(a)) = (-P_m(a)^2 / Q_k(a))$$
$$= -1 \text{ by (1.16)}$$

Thus $P_n(a) \neq P_m(a)Y^2$.

This completes the proof.

THEOREM 1.8. For any given m such that $|P_m(a)| > 2$, $P_n(a)$ is of the form $2P_m(a)Y^2$ only for $n = 0$, ($a = 1$ or 5, $m = 6$, $n = 12$) and ($a = 1$ or 5, $m = -6$, $n = -12$).

Proof. We note first from corollary 1.1 that if $P_n(a) = 2P_m(a)Y^2$, then $n = mt$ for some integer t.

(i) Suppose that t is even. Let $t = 2t'$. Then by (1.8) and (1.13) as before

$$P_n(a) = P_{mt'}(a)\, Q_{mt'}(a)$$

where $(P_{mt'}(a), Q_{mt'}(a)) = 1$ or 2. Also $P_m(a) \mid P_{mt'}(a)$ by lemma 1.1. Hence, if $P_n(a) = 2P_m(a)Y^2$ we require either

$$P_{mt'}(a) = 2P_m(a)Y_1^2 \; ; \quad Q_{mt'}(a) = Y_2^2$$

where from theorem 1.1 the only possible solution is $Q_3(3) = Y_2^2$, or

$$P_{mt'}(a) = P_m(a)Y_1^2 \; ; \quad Q_{mt'}(a) = 2Y_2^2$$

From theorem 1.2 the only possible solutions here are $Q_o(a) = 2$, $Q_{\pm 6}(1) = 2Y_2^2$, $Q_{\pm 6}(5) = 2Y_2^2$.

These possibilities lead only to the solutions $n = 0$, ($a = 1$ or 5, $m = 6$, $n = 12$) and ($a = 1$ or 5, $m = -6$, $n = -12$) since the equation $P_3(3) = 2P_m(3)Y_1^2$ has no solution.

(ii) Suppose that t is odd but m is even. Put $m = 2m'$. Then as before we can easily show that we require either

$$P_{m't}(a) = P_{m'}(a)Y_1^2 \; ; \quad Q_{m't}(a) = 2Q_{m'}(a)Y_2^2$$

where from theorem 1.6 the second equation has no solution, or

$$P_{m't}(a) = 2P_{m'}(a)Y_1^2 \; ; \quad Q_{m't}(a) = Q_{m'}(a)Y_2^2$$

From theorem 1.5 the second equation requires $t = \pm 1$, but $P_{m'}(a) \neq 2P_{m'}(a)Y_1^2$.

(iii) Suppose that m and t are both odd and $3 \nmid m$. From (1.12), if $P_n(a) = 2P_m(a)Y^2$, $3 \mid n$. Thus $3 \mid t$. Put $t = 3t'$. Then from (1.8) and (1.10)

$$\begin{aligned} P_n(a) = P_{3t'm}(a) &= P_{t'm}(a) \; (Q_{t'm}(a)^2 + 1) \\ &= P_{t'm}(a) \left((a^2 + 4)P_{t'm}(a)^2 - 3 \right) \text{ by (1.11)} \end{aligned}$$

since mt' is odd. Thus $(P_{t'm}(a), Q_{t'm}(a)^2 + 1) = 1$ or 3.

But $Q_{t',m}(a)^2 + 1$ is not divisible by 3 and so $(P_{t',m}(a), Q_{t',m}(a)^2 + 1) = 1$. By lemma 1.1 $P_m(a) \mid P_{t',m}(a)$ and so if $P_n(a) = 2P_m(a)Y^2$ we need either

$$P_{t',m}(a) = 2P_m(a)Y_1^2 \; ; \; Q_{t',m}(a)^2 + 1 = Y_2^2$$

where the second equation is impossible, or

$$P_{t',m}(a) = P_m(a)Y_2^2 \; ; \; Q_{t',m}(a)^2 + 1 = 2Y_2^2$$

From the first equation by theorem 1.7 $t' = 1$ and from the second by (1.31) since m is odd and $3 \nmid m$, $m = \pm 1$. But if $m = \pm 1$, $|P_m(a)| < 2$.

Thus $P_n(a) \neq 2P_m(a)Y^2$ in this case.

(iv) Suppose finally that m and t are both odd and $3 \mid m$. Then $3 \mid n$ also and from (1.14) and the first 12 values of $P_r(a)$ we find that

$$2 \mid P_m(a), \; 4 \nmid P_m(a) \; ; \; 2 \mid P_n(a), \; 4 \nmid P_n(a).$$

Hence $P_n(a) \neq 2P_m(a)Y^2$.

This completes the proof.

THEOREM 1.9. For any given m such that $|Q_m(a)| > 2$, $P_n(a)$ is of the form $Q_m(a)Y^2$ only for ($a > 2$, $m = 1$, $n = 2$), ($a > 2$, $m = -1$, $n = -2$), ($a = 1$, $m = \pm 12$, $n = 24$), ($a = 1$, $m = 3$, $n = 12$), ($a = 1$, $m = -3$, $n = -12$) and (a = a perfect square, $m = \pm 2$, $n = 4$).

Proof. From corollary 1.1 we first note that if $P_n(a) = Q_m(a)Y^2$, then $n = 2mt$ for some integer t. Then by (1.8) we have

$$P_n(a) = P_{mt}(a) \, Q_{mt}(a) \qquad (***)$$

(i) Suppose first that t is odd. Then by lemma 1.2 $Q_m(a) \mid Q_{mt}(a)$. From (1.13) $(P_{mt}(a), Q_{mt}(a)) = 1$ or 2, and so if $P_n(a) = Q_m(a)Y^2$ we require either

$$P_{mt}(a) = 2Y_1^2 \; ; \quad Q_{mt}(a) = 2Q_m(a)Y_2^2$$

where from theorem 1.6 the second equation has no solutions, or

$$P_{mt}(a) = Y_1^2 \; ; \quad Q_{mt}(a) = Q_m(a)Y_2^2$$

From theorem 1.5 the only possibilities for the second equation are $t = \pm 1$. From theorem 1.3 and the first equation we then find that the only solutions are

$P_{24}(1) = 12^2.Q_{\pm 12}(1)$; $P_2(a) = Q_1(a).1^2$, $a > 2$;
$P_{-2}(a) = Q_{-1}(a).1^2$, $a > 2$; $P_4(a) = Q_{\pm 2}(a).\, a$, a a perfect square.

(ii) Suppose now that t is even. Then from lemma 1.1 and (1.8) we have

$$P_{2m}(a) = P_m(a)\, Q_m(a) \mid P_{tm}(a)$$

and so, by virtue of (1.13) and (***) we require either

$$P_{mt}(a) = Q_m(a)Y_1^2 \; ; \quad Q_{mt}(a) = Y_2^2$$

where from theorem 1.1, since t is even the second equation has no solutions, or

$$P_{mt}(a) = 2Q_m(a)Y_1^2 \; ; \; Q_{mt}(a) = 2Y_2^2$$

where from theorem 1.2 the only solutions of the second equation are $mt = \pm 6$, $a = 1$ or 5. These possibilities yield only the solutions $P_{12}(1) = Q_3(1).6^2$; $P_{-12}(1) = Q_{-3}(1).6^2$.
This completes the proof.

THEOREM 1.10. For any given m such that $|Q_m(a)| > 2$, $P_n(a)$

is of the form $2Q_m(a)Y^2$ only for ($a = 1$, $m = \pm 6$, $n = 12$), ($a = \frac{1}{2}Q_{2n+1}(2)$, $m = 3$, $n = 6$) and ($a = \frac{1}{2}Q_{2n+1}(2)$, $m = -3$, $n = -6$).

Proof. Again we note that from corollary 1.1 if $P_n(a) = 2Q_m(a)Y^2$, then $n = 2mt$ for some integer t. From (1.8) and (1.13) we have

$$P_n(a) = P_{mt}(a)\, Q_{mt}(a) \qquad (***)$$

and $(P_{mt}(a), Q_{mt}(a)) = 1$ or 2.

(i) Suppose that t is odd. Then from lemma 1.2 $Q_m(a) | Q_{mt}(a)$ and so, if $P_n(a) = 2Q_m(a)Y^2$ we require either

$$P_{mt}(a) = Y_1^2 \; ; \quad Q_{mt}(a) = 2Q_m(a)Y_2^2$$

where, from theorem 1.6 the second equation has no solutions, or

$$P_{mt}(a) = 2Y_1^2 \; ; \quad Q_{mt}(a) = Q_m(a)Y_2^2$$

From theorem 1.5 the only solutions of the second equation are $t = \pm 1$. From the first equation and theorem 1.4 we find that the only solutions are

$$P_{12}(1) = 2Q_{\pm 6}(1).2^2; \; P_6\left(\tfrac{1}{2}Q_{2n+1}(2)\right) = 2Q_3\left(\tfrac{1}{2}Q_{2n+1}(2)\right).Y^2;$$

$$P_{-6}\left(\tfrac{1}{2}Q_{2n+1}(2)\right) = 2Q_{-3}\left(\tfrac{1}{2}Q_{2n+1}(2)\right).Y^2.$$

(ii) Suppose now that t is even. Then from (1.8) and lemma 1.1

$$P_{2m}(a) = P_m(a)\, Q_m(a) \mid P_{mt}(a)$$

and so from (***) we require either

$$P_{mt}(a) = 2Q_m(a)Y_1^2 \; ; \; Q_{mt}(a) = Y_2^2$$

where from theorem 1.1 since t is even the second equation

has no solutions, or

$$P_{mt}(a) = Q_m(a)Y_1^2 \; ; \; Q_{mt}(a) = 2Y_2^2$$

where from theorem 1.2 the only possible solutions for the second equation are $mt = \pm 6$, $a = 1$ or 5. However these values give no solutions for the first equation.

This completes the proof.

THEOREM 1.11. For any given m such that $|P_m(a)| > 2$, $Q_n(a)$ is of the form $P_m(a)X^2$ only for ($a > 2$, $m = 2$, $n = 1$) and ($a = 1$, $m = 4$, $n = \pm 2$).

Proof. From corollary 1.1 we see that if $Q_n(a) = P_m(a)X^2$ then $m = 2$, $a > 2$ or $m = 4$, $a = 1$.

Now $P_2(a) = Q_1(a)$ and therefore from theorem 1.5 $Q_n(a) = P_2(a)X^2$ if and only if $n = 1$.

Similarly $P_4(1) = Q_{\pm 2}(1)$ and so by theorem 1.5 $Q_n(1) = P_4(1)X^2$ if and only if $n = \pm 2$.

This completes the proof.

THEOREM 1.12. For any given m such that $|P_m(a)| > 2$, $Q_n(a)$ is never of the form $2P_m(a)X^2$.

Proof. From corollary 1.1 we see that if $Q_n(a) = 2P_m(a)X^2$ then $m = 2$, $a > 2$ or $m = 4$, $a = 1$.

But $P_2(a) = Q_1(a)$ and $P_4(1) = Q_{\pm 2}(1)$ and the result follows from theorem 1.6.

The following results will be required later and are a direct consequence of theorems 1.1 - 1.12.

COROLLARY 1.2. (Of theorems 1.1 - 1.12).

(a) If $|P_m(a)| \geq |P_n(a)| > 2$, $P_m(a)\,P_n(a)$ is a square only for $m = n$ if n is even, $m = \pm n$ if n is odd and ($a = 3$, $m = 6$, $n = \pm 3$). $2P_m(a)\,P_n(a)$ is a square only for ($a = 1$, or 5, $m = 12$, $n = 6$)

($a = 1$ or 5, $m = -12$, $n = -6$) and ($a = \frac{1}{2}Q_{2n+1}(2)$ = a perfect square $\neq 1$, $m = \pm 3$, $n = 2$)

(b) If $|Q_m(a)| \geq |Q_n(a)| > 2$, $Q_m(a)\, Q_n(a)$ is a square only for $m = n$ if n is odd and $m = \pm n$ if n is even. $2Q_m(a)\, Q_n(a)$ is a square only for ($a = 1$, $m = \pm 6$, $n = 3$).

(c) If $|P_n(a)| > 2$, $|Q_m(a)| > 2$, $P_n(a)\, Q_m(a)$ is a square only for ($a > 2$, $m = 1$, $n = 2$), ($a > 2$, $m = -1$, $n = -1$), ($a = 1$, $m = \pm 12$, $n = 24$), ($a = 1$, $m = \pm 6$, $n = 6$), ($a = 1$, $m = 3$, $n = 12$), ($a = 1$, $m = -3$, $n \neq -12$) and (a = a perfect square, $m = \pm 2$, $n = 4$). $2P_n(a)\, Q_m(a)$ is a square only for ($a = 1$, $m = 3$, $n = 6$), ($a = 1$, $m = \pm 6$, $n = 12$), ($a = \frac{1}{2}Q_{2n+1}(2)$, $m = 3$, $n = 6$), ($a = \frac{1}{2}Q_{2n+1}(2)$ $m = -3$, $n = -6$) and ($a = \frac{1}{2}Q_{2n+1}(2)$ = a perfect square $\neq 1$, $m = 1$, $n = \pm 3$).

Proof.(a) From lemma 1.4 $(P_m(a), P_n(a)) = P_{(m,n)}(a)$ and, therefore, if $P_m(a)\, P_n(a) = Y^2$, we must have $P_m(a) = P_{(m,n)}(a)Y_1^2$, $P_n(a) = P_{(m,n)}(a)Y_2^2$. If $|P_{(m,n)}(a)| > 2$ from theorem 1.7 we require $m = (m,n) = n$ if n is even, $m = \pm(m,n)$, $n = \pm(m,n)$ if n is odd, or ($a = 3$, $m = 6$, $(m,n) = n = \pm 3$). If $|P_{(m,n)}(a)| = 1$ or 2 from theorems 1.3 and 1.4 the only possibility is $m = n = 2$.

Similarly $2P_m(a)\, P_n(a) = Y^2$ implies that either

$$P_m(a) = P_{(m,n)}(a)Y_1^2 \; ; \quad P_n(a) = 2P_{(m,n)}(a)Y_2^2$$

or

$$P_m(a) = 2P_{(m,n)}(a)Y_1^2 \; ; \quad P_n(a) = P_{(m,n)}(a)Y_2^2$$

If $|P_{(m,n)}(a)| > 2$ from theorems 1.7 and 1.8 this is possible only for ($a = 1$ or 5, $m = 12$, $n = 6$) and ($a = 1$ or 5, $m = -12$, $n = -6$). If $|P_{(m,n)}(a)| = 1$ or 2 theorems 1.3 and 1.4 give only one more solution ($a = \frac{1}{2}Q_{2n+1}(2)$ = a perfect square $\neq 1$,

$m = \pm 3$, $n = 2$).

The proofs of (b) and (c) follow similarly from theorems 1.1 - 1.12.

We have now solved the equations $P_n(a) = NY^2$, $Q_n(a) = NX^2$ in the cases $N = P_m(a)$, $2P_m(a)$, $Q_m(a)$ and $2Q_m(a)$. We wish to solve them for general square-free values of N but it is convenient to consider one more special case before proceeding to the solution in the general case. Here again we do not confine ourselves to square-free values.

It is obvious from (1.11) that since a is odd $(Q_n(a), a^2 + 4) = 1$ and that therefore if $Q_n(a) = RX^2$ and $R \mid a^2 + 4$, then $R = 1$. The following two results, however, are not so trivial.

THEOREM 1.13. Let R be an integer greater than 1 such that $R \mid a^2 + 4$. Then the equation $P_n(a) = RY^2$ has no solutions other than $n = 0$ and ($R = \pm 5$, $n = \pm 5$, $a = 1$).

Proof. From (1.26) and (1.27) we see that $R \mid P_n(a)$ if and only if $R \mid n$. If $P_n(a) = RY^2$, therefore, $n = mR$ for some integer m.

(i) Suppose first that m is even. Then from (1.8)

$$P_n(a) = P_{\frac{1}{2}mR}(a)\, Q_{\frac{1}{2}mR}(a)$$

where $R \mid \frac{1}{2}mR$ and therefore $R \mid P_{\frac{1}{2}mR}(a)$ from (1.26) and (1.27). Thus by virtue of (1.13) if $P_n(a) = RY^2$ we require either

$$P_{\frac{1}{2}mR}(a) = RY_1^2 \; ; \; Q_{\frac{1}{2}mR}(a) = Y_2^2$$

where, since $R > 1$ from theorem 1.1 the only possibility is $\frac{1}{2}mR = 3$, or

$$P_{\frac{1}{2}mR}(a) = 2RY_1^2 \; ; \; Q_{\frac{1}{2}mR}(a) = 2Y_2^2$$

The latter equation from theorem 1.2 requires $\frac{1}{2}mR = 0, \pm 6$.

Clearly $P_o(a) = R.0^2$ but, since $R > 1$, all the other possibilities require $R = \pm 2, \pm 3, \pm 6$ and since $R \mid a^2 + 4$ where a is odd these are all impossible.

(ii) Suppose now that m is odd. Since $R \mid a^2 + 4$, $R \equiv 1 \pmod 4$. If $R \equiv 1 \pmod 8$ we write $mR = \pm 1 + 2.3^r.k$ where $2 \mid k$, $3 \nmid k$. Then repeated applications of (1.21) give

$$P_{mR}(a) \equiv (-1)^{3^r} P_{\pm 1}(a) \pmod{Q_k(a)}$$

$$\equiv -1 \text{ by (1.6)}$$

From (1.24), since R is odd and $2 \mid k$ therefore

$$\begin{aligned}(RP_{mR}(a) / Q_k(a)) &= (-R / Q_k(a)) = -(R / Q_k(a)) \text{ by (1.16)} \\ &= -(Q_k(a) / R) \text{ since } R \equiv 1 \pmod 4 \\ &= -(\pm 2 / R) \text{ by (1.24) since } 2 \mid k \\ &= -1 \text{ since } R \equiv 1 \pmod 8\end{aligned}$$

Thus $P_{mR}(a) \neq RY^2$.

If $R \equiv 5 \pmod 8$ and $mR \neq \pm 5$ we may write $mR = \pm 5 + 2.3^r.5^s.k$ where $2 \mid k$, $3 \nmid k$, $5 \nmid k$. Thus if $|mR| \neq 5$ from (1.21) we obtain

$$P_{mR}(a) \equiv -P_{\pm 5}(a) \pmod{Q_k(a)}$$

But now since $5 \nmid k$ from (1.20) and (1.7) we find that

$$Q_k(a) \equiv -Q_{k-10}(a) \equiv \cdots \equiv \pm Q_2(a) \text{ or } \pm Q_4(a) \pmod{RP_5(a)}$$

Also

$$\begin{aligned}(Q_2(a) / RP_5(a))(Q_4(a) / RP_5(a)) &= (Q_2(a)Q_4(a) / R) \times \\ &\quad (Q_2(a)Q_4(a) / P_5(a)) \\ &= (-4 / R)\big((a^2 + 2) \times \\ &\quad (a^4 + 4a^2 + 2)/a^4 + 3a^2 + 1\big) \\ &\quad \text{by (1.24)}\end{aligned}$$

$$= (1 + (a^4 + 3a^2 + 1)(a^2 + 3) / a^4 + 3a^2 + 1)$$

Since $R \equiv 1 \pmod 4$

$$= 1.$$

Thus $(Q_2(a) / RP_5(a)) = (Q_4(a) / RP_5(a))$

Hence we find that

$$\begin{aligned}(RP_{mR}(a) / Q_k(a)) &= (-RP_{\pm 5}(a) / Q_k(a)) \\ &= -(Q_k(a) / RP_5(a)) \text{ by (1.16) and (1.6),} \\ &\qquad \text{since } RP_5(a) \equiv 1 \pmod 4. \\ &= -(\pm Q_2(a) / RP_5(a)) \text{ from the above} \\ &= -(a^2 + 2 / RP_5(a)) \text{ since } RP_5(a) \equiv 1 \pmod 4 \\ &= -(-2/R)(a^4 + 3a^2 + 1 / a^2 + 2) \\ &= (-1 / a^2 + 2) \text{ since } R \equiv 5 \pmod 8 \\ &= -1 \text{ since } a^2 + 2 \equiv 3 \pmod 4\end{aligned}$$

Thus again $P_{mR}(a) \neq RY^2$.

Therefore, if $P_{mR}(a) = RY^2$, $mR = \pm 5$. But since $R > 1$ this implies that $R = 5$, $m = \pm 1$.

(iii) Let $P_5(a) = P_{-5}(a) = 5Y^2$. Then

$$a^4 + 3a^2 + 1 = 5Y^2.$$

or

$$(2a^2 + 3)^2 - 5 = 20Y^2.$$

Thus $5 \mid 2a^2 + 3$ and

$$(2Y)^2 - 5\left(\frac{2a^2 + 3}{5}\right)^2 = -1$$

But from (1.11) we see that this implies that

$$2\left(\frac{2a^2+3}{5}\right) = P_{2n+1}(1)$$

for some n, i.e.

$$(2a)^2 = 5P_{(2n+1)}(1) - 6$$

We show that this equation has only the solutions $2n+1 = \pm 3$. If $2n+1 = \pm 3$, $5P_{2n+1}(1) - 6 = 10 - 6 = 4$, whereas if $2n+1 \neq \pm 3$ we may write $2n+1 = \pm 3 + 2.3^r.k$ as before and from (1.21) we obtain

$$5P_{2n+1}(1) - 6 \equiv -5P_{\pm 3}(1) - 6 \equiv -16 \pmod{Q_k(1)}$$

From (1.16) therefore

$$(5P_{2n+1}(1) - 6 \,/\, Q_k(1)) = -1$$

Hence the result. This then implies that the only solution of

$$a^4 + 3a^2 + 1 = 5Y^2$$

is $a = 1$, $Y = \pm 1$.

This completes the proof.

THEOREM 1.14. Let R be an integer greater than 1 such that $R \mid a^2 + 4$. Then the equation $P_n(a) = 2RY^2$ has no solutions other than $n = 0$.

Proof. From (1.26) and (1.27) we again see that $R \mid P_n(a)$ if and only if $R \mid n$. Now $3 \nmid R$ since $R \mid a^2 + 4$ and therefore, from (1.12) we find that $2R \mid P_n(a)$ if and only if $3R \mid n$. Let $n = 3Rm$.

(i) Suppose first that m is even. Then from (1.8)

$$P_{3Rm}(a) = P_{3Rm/2}(a)\, Q_{3Rm/2}(a)$$

and from (1.26) and (1.27) $R \mid P_{3Rm/2}(a)$. Hence if $P_{3Rm}(a) = 2RY^2$, we require

$$Q_{3Rm/2}(a) = Y_1^2 \text{ or } 2Y_1^2,$$

From theorems 1.1 and 1.2 the only possibilities are $3R\frac{m}{2} = 0, 3$ or 6. Since $R \mid a^2 + 4$, $R > 1$, $3R(\frac{1}{2}m) = 3$ or 6 is impossible and we have only the solution $n = 0$.

(ii) Suppose now that m is odd. Then from (1.8) and (1.10)

$$P_{3Rm}(a) = P_{Rm}(a)\,(Q_{Rm}(a)^2 + 1)$$

where from (1.11) $(P_{Rm}(a), Q_{Rm}(a)^2 + 1) = 1$ or 3. But $3 \nmid Q_{Rm}(a)^2 + 1$ and therefore $(P_{Rm}(a), Q_{Rm}(a)^2 + 1) = 1$. Also, from (1.27) $R \mid P_{Rm}(a)$. Thus if $P_{3Rm}(a) = 2RY^2$ we require either

$$Q_{Rm}(a)^2 + 1 = Y_1^2$$

which is impossible, or

$$Q_{Rm}(a)^2 + 1 = 2Y_1^2$$

which implies $Q_{Rm}(a)$ is odd. Hence from (1.12) $3 \nmid mR$. Since also $2 \nmid mR$ from (1.31) the only possibilities are $Rm = \pm 1$. But $R > 1$ and so there are no solutions.

This completes the proof.

We have now proved all the preliminary results which we need in order to solve the equations $P_n(a) = NY^2$ and $Q_n(a) = NX^2$ for general square-free values of N. We begin the final part of this chapter by proving that in general these equations have at most one solution. Since $P_{-n}(a) = \pm P_n(a)$ and $Q_{-n}(a) = \pm Q_n(a)$ we consider only positive values of n. We prove

THEOREM 1.15. The equations

$$\left.\begin{array}{ll} 1. & P_r(a) = NY_1^2 \\ 2. & P_s(a) = 2NY_2^2 \\ 3. & Q_t(a) = NX_1^2 \\ 4. & Q_u(a) = 2NX_2^2 \end{array}\right\}$$

where r, s, t and u are positive integers,

have each at most one solution for any given square-free odd integer $N>1$, except in the case $a = 3$, $N = 5$ when equation 2 has solutions $s = 3$ and $s = 6$.

If one of these four equations has a solution there are no solutions of the other three except in the cases

(i) $a > 2, a = NK^2$, N square-free, when

$$P_2(a) = NK^2$$
$$Q_1(a) = NK^2$$

(ii) $a = 1$, when

$$P_{24}(a) = 2.161.12^2$$
$$Q_{12}(a) = 2.161.1^2$$

(iii) $a = R^2$, $a^2 + 2 = NK^2$, N square-free, when

$$P_4(a) = N.(RK)^2$$
$$Q_2(a) = N.K^2$$

(iv) $a = \frac{1}{2}Q_{2n+1}(2)$, $a^2 + 1 = 2R^2$, $a^3 + 3a = NK^2$, N square-free, when

$$Q_3(a) = NK^2$$
$$P_6(a) = 2.N.(RK)^2$$

(v) $a = 5$ when $P_6(a) = 2.455.2^2$, $P_{12}(a) = 455.396^2$.

Proof. If $P_r(a) = NY_1^2$ has two solutions m and n, then $P_n(a)\,P_m(a) = NY_1^2 . NY'^2_1 = T^2$, say, and from corollary 1.2 we must have $a = 3$, $m = 6$, $n = 3$. But $P_3(3) = 10$ and so $P_3(3) \neq NY^2$ where N is odd and so the equation $P_r(a) = NY^2$ has at most one solution for any given odd square-free integer N.

Similarly, if $P_s(a) = 2NY^2$ has two solutions m and n, say, then $P_m(a)\,P_n(a)$ is a square and from corollary 1.2 the only solution is $a = 3,\ m = 6,\ n = 3,\ N = 5$.

The other parts of the theorem follow in a similar way from corollary 1.2.

Thus, in general, the equations 1 - 4 of theorem 1.15 have at most one solution between them. We now proceed to the problem of determining this one solution if it exists. It is convenient to distinguish, as in theorem 1.15 between an odd and an even square-free integer. Thus, from now on, N will denote an odd square-free integer.

We need first to consider when a given N will divide $P_n(a)$ or $Q_n(a)$.

Let h_r be the least non-negative residue of $P_r(a)$ modulo R where R is any integer. Since there are only R residues modulo R there are only R^2 possibilities for the pair of integers (h_r, h_{r+1}). Hence there exist integers m and n such that $h_m = h_n$, $h_{m+1} = h_{n+1}$, and $m \neq n$. But then, since $P_r(a)$ satisfies a three-term recurrence relation

$$h_{m+t} = h_{n+t}$$

for all integers t. In particular

$$0 = h_o = h_{m-m} = h_{n-m}$$

i.e. $R \mid P_{n-m}(a)$.

Thus any integer R will divide $P_r(a)$ for some non-zero value of r. It is not necessarily true, however, that R divides $Q_r(a)$ for some r, e.g. it is easily seen that $5 \nmid Q_r(1)$ for any integer r. Hence we make the following definitions.

DEFINITION. The rank of apparition of the integer R with

respect to the sequence $P_r(a)$ is the least positive value of r for which $R \mid P_r(a)$.

DEFINITION. If the integer R divides $Q_r(a)$ for some value of r, the rank of apparition of R with respect to the sequence $Q_r(a)$ is the least positive value of r for which $R \mid Q_r(a)$. If R does not divide $Q_r(a)$ for any value of r then the rank of apparition of R with respect to the sequence $Q_r(a)$ is not defined.

The following two lemmas are a direct consequence of the definitions.

LEMMA 1.7. If ρ is the rank of apparition of R with respect to the sequence $P_r(a)$, then $R \mid P_n(a)$ if and only if $\rho \mid n$.

Proof. From lemma 1.1 clearly $R \mid P_n(a)$ if $\rho \mid n$. Suppose now that $R \mid P_n(a)$. Then $R \mid (P_\rho(a), P_n(a))$, i.e. from lemma 1.4 $R \mid P_{(n,\rho)}(a)$. Thus, from the definition of ρ, $(n,\rho) \geq \rho$. But clearly $(n,\rho) \leq \rho$. Thus $(n,\rho) = \rho$, i.e. $\rho \mid n$.

Lemma 1.8. If $R > 2$ is an integer such that the rank of apparition, ρ, of R with respect to the sequence $Q_r(a)$ is defined, then $R \mid Q_n(a)$ if and only if $n = s\rho$ where s is an odd integer.

Proof. From lemma 1.2 clearly $R \mid Q_n(a)$ if $n = s\rho$ where s is odd. Suppose now that $R \mid Q_n(a)$. Then $R \mid (Q_n(a), Q_\rho(a)) = 2$ or $Q_{(n,\rho)}(a)$ from lemma 1.5. Since $R > 2$ we must have $(Q_n(a), Q_\rho(a)) = Q_{(n,\rho)}(a)$. Thus, from the definition of ρ, $(n,\rho) \geq \rho$. But clearly $(n,\rho) \leq \rho$, i.e. $(n,\rho) = \rho$. But then, from lemma 1.5, since $(Q_n(a), Q_\rho(a)) = Q_{(n,\rho)}(a)$, $\frac{n}{\rho}$ must be odd. i.e. $n = s\rho$ where s is odd.

We are now able to proceed to the main results which are contained in the final four theorems, theorems 1.16 - 1.19.

THEOREM 1.16. Let N be a positive odd square-free integer whose rank of apparition, ρ, with respect to the sequence $Q_n(a)$

is defined.

Then

(a) If $2\nmid\rho$, $3\nmid\rho$, $Q_n(a) = NX^2$ can occur only if $n = \rho$.

(b) If $2\mid\rho$, $3\nmid\rho$, $Q_n(a) = NX^2$ can occur only if $n = \pm\rho$ and $N \equiv 3 \pmod 4$

(c) If $2\nmid\rho$, $3\mid\rho$, $Q_n(a) = NX^2$ can occur only if $n = \rho$.

(d) If $2\mid\rho$, $3\mid\rho$, $Q_n(a) = NX^2$ has no solutions.

Proof. From lemma 1.8 we see first that if $Q_n(a) = NX^2$, then $n = r\rho$ for some odd integer r.

(a) Suppose that $2\nmid\rho$, $3\nmid\rho$. Then if $Q_\rho(a) = NX^2$, from theorem 1.15 and (1.7) $Q_{r\rho}(a) \neq NX^2$ for any $r \neq 1$. If $Q_\rho(a) \neq NX^2$, $Q_\rho(a) = N.R.x^2$ for some square-free integer R, $R > 1$. Since $3\nmid\rho$, from (1.12) R and x are odd. Since $2\nmid\rho$, from (1.33) for all r

$$Q_{r\rho}(a) = Q_r\left(Q_\rho(a)\right).$$

Thus if $Q_{r\rho}(a) = NX^2$, we require $Q_r\left(Q_\rho(a)\right) = NX^2$.

(i) Suppose first that $R \equiv 1$ or $3 \pmod 8$. Then, since $r \neq 1$, $r = 3$ or we may write $r = t + 2.3^s.k$ where $2\mid k$, $3\nmid k$, and $t = 1$ or 3. Since $Q_\rho(a)$ is odd, from (1.22) we now find

$$Q_r\left(Q_\rho(a)\right) \equiv (-1)^{3^s} Q_t\left(Q_\rho(a)\right) \pmod{Q_k\left(Q_\rho(a)\right)}$$

where, from lemma 1.5, since $2\mid k$, $3\nmid k$, $\left(Q_k\left(Q_\rho(a)\right), Q_t\left(Q_\rho(a)\right)\right) = 1$. Thus, from (1.30) with $n = 1$,

$$\begin{aligned}\left(NQ_{r\rho}(a) \,/\, Q_k\left(Q_\rho(a)\right)\right) &= \left(-NQ_\rho(a) \,/\, Q_k\left(Q_\rho(a)\right)\right)\\ &= \left(-N^2.R.x^2 \,/\, Q_k\left(Q_\rho(a)\right)\right)\\ &= -\left(R \,/\, Q_k\left(Q_\rho(a)\right)\right) \text{ by (1.16)}\\ &= -\left(-Q_k\left(Q_\rho(a)\right) \,/\, R\right) \text{ by (1.16)}\end{aligned}$$

But now, by (1.23) since $2\mid k$, $Q_k\left(Q_\rho(a)\right) \equiv 2 \pmod{Q_\rho(a)}$. Hence

$Q_k\left(Q_\rho(a)\right) \equiv 2 \pmod{R}$. Thus

$$\left(NQ_{r\rho}(a) \,/\, Q_k\left(Q_\rho(a)\right)\right) = -(-2 \,/\, R) = -1 \text{ since } R \equiv 1 \text{ or } 3 \pmod 8.$$

Thus $Q_{r\rho}(a) \neq NX^2$ except possibly if $r = 1$ or 3.

(ii) Suppose now that $R \equiv 5$ or 7, (mod 8). Then, since $2 \nmid r\rho$, from (1.7) we may suppose that r is positive and so we may write $r = t + 2.3^s.k$ where $2 \mid k$, $3 \nmid k$, and $t = -1$ or -3. Then as above, by repeated applications of (1.22) we have

$$Q_{r\rho}(a) \equiv -Q_t\left(Q_\rho(a)\right) \pmod{Q_k\left(Q_\rho(a)\right)}$$

Thus again, from lemma 1.5 and (1.30)

$$\begin{aligned}\left(NQ_{r\rho}(a) \,/\, Q_k\left(Q_\rho(a)\right)\right) &= \left(NQ_\rho(a) \,/\, Q_k\left(Q_\rho(a)\right)\right)\\ &= \left(N^2.R.x^2 \,/\, Q_k\left(Q_\rho(a)\right)\right)\\ &= \left(-Q_k\left(Q_\rho(a)\right) \,/\, R\right) \text{ by (1.16)}\\ &= (-2 \,/\, R) \text{ by (1.23)}\\ &= -1 \text{ since } R \equiv 5 \text{ or } 7 \pmod 8.\end{aligned}$$

Thus again $Q_{r\rho}(a) \neq NX^2$ except possibly for $r = 1$ or 3.

(iii) Suppose finally that $r = 3$. Then from (1.23)

$$NX^2 = Q_{3\rho}(a) = Q_3\left(Q_\rho(a)\right) = Q_\rho(a)\left(Q_\rho(a)^2 + 3\right)$$

where $\left(Q_\rho(a),\ Q_\rho(a)^2 + 3\right) = 1$ or 3 and $N \mid Q_\rho(a)$. Thus we must have either

$$Q_\rho(a)^2 + 3 = Y_1^2$$

which is impossible since $\left|Q_\rho(a)\right| > 1$, or

$$Q_\rho(a)^2 + 3 = 3Y_1^2$$

whence, since ρ is odd, from (1.10)

$$Q_{2\rho}(a) = 3Y_1^2 - 1.$$

Now $2\rho = 2.3^s.k \pm 2$ where $4|k$, $3\nmid k$, and from (1.22)

$$3Y_1^2 - 1 \equiv -Q_{\pm 2}(a) \pmod{Q_k(a)}$$

$$\equiv -(a^2 + 2) \pmod{Q_k(a)}$$

Thus

$$-3Y_1^2 \equiv a^2 + 1 \pmod{Q_k(a)}$$

But now either $3|a = Q_1(a)$ or $3|a^2 + 2 = Q_2(a)$ and since we require $3|Q_\rho(a)$ where ρ is odd, from lemma 1.5 clearly $3\nmid a^2 + 2$. so $3|a$. From (1.23), therefore, $Q_k(a) \equiv 2 \pmod 3$. Also, since $4|k$, $Q_k(a) \equiv 7 \pmod 8$ by (1.16). Now $a^2 + 1 = P_3(a)$ and so, from lemma 1.6, $(Q_k(a), a^2 + 1) = 1$. Also $\frac{1}{2}(a^2 + 1) \equiv 1 \pmod 4$. Thus

$$\begin{aligned}(-3Y_1^2 / Q_k(a)) = (-3 / Q_k(a)) &= (2 / 3)\\ &= -1\\ &= (\tfrac{1}{2}(a^2 + 1) / Q_k(a))(2/Q_k(a))\\ &= (Q_k(a) / \tfrac{1}{2}(a^2 + 1))\end{aligned}$$

But since $k \equiv \pm 2 \pmod 6$, from (1.20)

$$Q_k(a) \equiv \pm Q_{\pm 2}(a) \pmod{\tfrac{1}{2}(a^2 + 1)}$$

$$\equiv \pm(a^2 + 2) \pmod{\tfrac{1}{2}(a^2 + 1)}$$

Thus

$$-1 = (\pm(a^2 + 2) / \tfrac{1}{2}(a^2 + 1)) = 1 \text{ since } \tfrac{1}{2}(a^2 + 1) \equiv 1 \pmod 4$$

which is clearly impossible.

Thus $Q_{3\rho}(a) \neq NX^2$.

This completes the proof of (a).

(b) Suppose that $2|\rho$, $3\nmid\rho$. Then if $Q_\rho(a) = NX^2$ by theorem 1.15 and (1.7) $Q_{r\rho}(a) \neq NX^2$ for any $r \neq \pm 1$. If $Q_\rho(a) \neq NX^2$, $Q_\rho(a) = N.R.x^2$ for some square-free integer R, $R > 1$. Since $3\nmid\rho$, from (1.12) R and x are odd.

(i) Suppose that $3\nmid r$. Then since r is odd and $3\nmid\rho$, $2|\rho$, from (1.16) $Q_{r\rho}(a) \equiv Q_\rho(a) \pmod 8$

Thus, since N is odd,

$$\frac{Q_{r\rho}(a)}{N} \equiv \frac{Q_\rho(a)}{N} \pmod 8$$

and so, if $Q_{r\rho}(a) = NX^2$, $R \equiv 1 \pmod 8$.

Now since $r \neq \pm 1$, we may write $r = \pm 1 + 2.3^s.k$ where $2|k$, $3\nmid k$.

Repeated applications of (1.22) now give

$$Q_{r\rho}(a) \equiv (-1)^{3^s}.Q_{\pm\rho}(a) \pmod{Q_{k\rho}(a)}$$

where, since $2|k\rho$, $3\nmid k\rho$, from lemma 1.5 $(Q_\rho(a), Q_{k\rho}(a)) = 1$.

Thus, by virtue of (1.7)

$$\begin{aligned}(NQ_{r\rho}(a) / Q_{k\rho}(a)) &= (NQ_\rho(a) / Q_{k\rho}(a)) \\ &= (N^2.R.x^2 / Q_{k\rho}(a)) \text{ by (1.16)} \\ &= -(Q_{k\rho}(a) / R) \text{ since } R \equiv 1 \pmod 8\end{aligned}$$

But from (1.18)

$$Q_{k\rho}(a) \equiv -Q_{(k-2)\rho}(a) \equiv \cdots \equiv \pm 2 \pmod{Q_\rho(a)}$$

Thus

$$(NQ_{r\rho}(a) / Q_{k\rho}(a)) = -(\pm 2 / R) = -1 \text{ since } R \equiv 1 \pmod 8$$

Thus $Q_{r\rho}(a) \neq NX^2$ if $3\nmid r$, $r \neq \pm 1$.

(ii) Suppose now that $r = 3r'$. Then from (1.8), (1.9) and (1.11)

$$Q_{r\rho}(a) = Q_{r'\rho}(a)\,(Q_{r'\rho}(a)^2 - 3)$$

where by lemma 1.8, $N \mid Q_{r'\rho}(a)$. Also $(Q_{r'\rho}(a), Q_{r'\rho}(a)^2 - 3) = 1$ or 3. Thus if $Q_{r\rho}(a) = NX^2$ we require either

$$Q_{r'\rho}(a)^2 - 3 = Y_1^2$$

which is impossible since $|Q_{r'\rho}(a)| > 2$, or

$$Q_{r'\rho}(a)^2 - 3 = 3Y_1^2$$

which is impossible modulo 9.

Now since $2 \mid \rho$, $3 \nmid \rho$, from (1.15) and the first twelve values of $Q_n(a)$, $Q_n(a) \equiv 3 \pmod 4$. Therefore $Q_n(a) \neq NX^2$ unless $N \equiv 3 \pmod 4$.

This completes the proof of (b).

(c) Suppose that $2 \nmid \rho$, $3 \mid \rho$. Then if $Q_\rho(a) = NX^2$, from theorem 1.15 and (1.7), $Q_{r\rho}(a) \neq NX^2$ for any $r \neq 1$. If $Q_\rho(a) \neq NX^2$, consider $Q_{r\rho}(a)$ for $r \neq \pm 1$.

(i) Suppose first that $3 \mid r$. Let $r = 3r'$. Then from (1.8), (1.9) and (1.11) we have

$$Q_{r\rho}(a) = Q_{r'\rho}(a)\left(Q_{r'\rho}(a)^2 + 3\right)$$

where $(Q_{r'\rho}(a), Q_{r'\rho}(a)^2 + 3) = 1$ or 3 and by lemma(1.8) $N \mid Q_{r'\rho}(a)$. Thus, if $Q_{r\rho}(a) = NX^2$ we require either

$$Q_{r'\rho}(a)^2 + 3 = Y_1^2$$

which is impossible since $|Q_{r'\rho}(a)| > 1$, or

$$Q_{r'\rho}(a)^2 + 3 = 3Y_1^2$$

But now, since $r'\rho$ is odd, as in the proof of (a) it is easily shown that this equation has no solutions.

Thus $Q_{3r'\rho}(a) \neq NX^2$.

(ii) Suppose now that $3\nmid r$. Then since $3\mid\rho$, from (1.8), (1.9) and (1.11) again, we have

$$Q_{r\rho}(a) = Q_{\frac{1}{3}r\rho}(a)\,(Q_{\frac{1}{3}r\rho}(a)^2 + 3)$$

where now $N \mid Q_\rho(a) = Q_{\frac{1}{3}\rho}(a)(Q_{\frac{1}{3}\rho}(a)^2 + 3)$. Let $N = N_1N_2$ where $N_1 \mid Q_{\frac{1}{3}\rho}(a)$, $N_2 \mid Q_{\frac{1}{3}\rho}(a)^2 + 3$ and if $3\mid N$, let $3\mid N_2$. From lemma 1.2, $N_1 \mid Q_{\frac{1}{3}r\rho}(a)$ and since $3\nmid r$, by lemma 1.5 $(Q_\rho(a), Q_{\frac{1}{3}r\rho}(a)) = Q_{\frac{1}{3}\rho}(a)$, giving $N_2 \mid Q_{\frac{1}{3}r\rho}(a)^2 + 3$.

Hence if $Q_{r\rho}(a) = NX^2$ we require

$$Q_{\frac{1}{3}r\rho}(a) = N_1X_1^2 \text{ or } 3N_1X_1^2$$

Now since $r\rho$ is odd, from lemma 1.5, if $3\mid Q_{\frac{1}{3}r\rho}(a)$, $3\nmid Q_2(a) = a^2 + 2$. Thus $3\mid a = Q_1(a)$, and so $3\mid Q_{\frac{1}{3}\rho}(a)$. Hence, if $3\mid Q_{\frac{1}{3}r\rho}(a)$, then $3\mid Q_{\frac{1}{3}\rho}(a)$. Therefore we require either

$$Q_{\frac{1}{3}r\rho}(a) = 3N_1X_1^2$$

where $3N_1 \mid Q_{\frac{1}{3}\rho}(a)$, or

$$Q_{\frac{1}{3}r\rho}(a) = N_1X_1^2$$

where $N_1 \mid Q_{\frac{1}{3}\rho}(a)$.

If $3\nmid \frac{1}{3}r\rho$, from (a) the first case is possible only for $r = 1$, and the second only for $r = 1$ or $N_1 = 1$. But if $N_1 = 1$, from theorem 1.1 since $3\nmid r$, again $r = 1$.

If $3\mid \frac{1}{3}r\rho$, we proceed as above until all factors of 3 in ρ are exhausted and eventually we see again from (a) and theorem 1.1 that there are no solutions for $r \neq 1$.

This completes the proof of (c).

(d) If $6 \mid \rho$, $6 \mid r\rho$, for all integers r. Thus $r\rho \equiv 0$ or $6 \pmod{12}$
Then from (1.15) and the first twelve values of $Q_n(a)$ we see that
$Q_{r\rho}(a) \equiv 2 \pmod 8$. Hence $Q_{r\rho}(a) \neq NX^2$ for any odd integer N.
This completes the proof of the theorem.

THEOREM 1.17. Let N be a positive odd square-free integer whose rank of apparition, ρ, with respect to the sequence $Q_n(a)$ is defined. Then $Q_n(a) = 2NX^2$ can occur only if $n = \pm\rho$, and $6 \mid \rho$.

Proof. We see first from lemma 1.8, that if $Q_n(a) = 2NX^2$ then $n = r\rho$ for some odd integer r. Also, from (1.12), if $Q_n(a) = 2NX^2$ then $3 \mid n$.

(i) Suppose first that $2 \nmid \rho$. Then $2 \nmid r\rho$, $3 \mid r\rho$, and from (1.15) and the first twelve values of $Q_n(a)$ we see that $Q_{r\rho}(a) \equiv 4 \pmod 8$. Thus $Q_{r\rho}(a) \neq 2NX^2$.

(ii) Suppose now that $2 \mid \rho$, and $3 \mid r$. Let $r = 3r'$. Then from (1.8), (1.9) and (1.11) if $Q_n(a) = 2NX^2$ we have

$$2NX^2 = Q_{r'\rho}(a)\,(Q_{r'\rho}(a)^2 - 3)$$

where $(Q_{r'\rho}(a),\ Q_{r'\rho}(a)^2 - 3) = 1$ or 3 and from lemma 1.8 $N \mid Q_{r'\rho}(a)$.
Thus we require

$$Q_{r'\rho}(a)^2 - 3 = X_1^2$$

which is impossible since $|Q_{r'\rho}(a)| > 2$, or

$$Q_{r'\rho}(a)^2 - 3 = 3X_1^2$$

which is impossible modulo 9, or

$$Q_{r'\rho}(a)^2 - 3 = 2X_1^2$$

which is impossible modulo 8, or

$$Q_{r'\rho}(a)^2 - 3 = 6X_1^2$$

Since $3|a = Q_1(a)$ or $3 | a^2 + 2 = Q_2(a)$ from lemma 3.5 we see that this last case can occur only if $3|a^2 + 2$ and $2|\rho r'$, $4\nmid \rho r'$.

If these conditions hold, from (1.10) we now have

$$Q_{2r'\rho}(a) = 6X_1^2 + 1$$

where $4|2r'\rho$, $8\nmid 2r'\rho$. Thus we may write $2r'\rho = \pm 4 + 2.3^s.k$ where $8|k$, $3\nmid k$. Repeated applications of (1.22) now give

$$6X_1^2 + 1 \equiv (-1)^{3^s} Q_{\pm 4}(a) \pmod{Q_k(a)}$$

$$\equiv -(a^4 + 4a^2 + 2) \pmod{Q_k(a)}$$

i.e.

$$6X_1^2 \equiv -(a^4 + 4a^2 + 3) \pmod{Q_k(a)}$$

Now $a^4 + 4a^2 + 3 \mid P_6(a)$ and so, from lemma 1.6, since $8|k$, $3\nmid k$ $(a^4 + 4a^2 + 3, Q_k(a)) = 1$. Also, from (1.20),

$$Q_k(a) \equiv Q_{k-12}(a) \equiv \cdots \equiv Q_{\pm 4}(a) \pmod{a^4 + 4a^2 + 3}$$

Since $8|k$, from (1.16) $Q_k(a) \equiv 7 \pmod 8$ and from (1.18) $Q_k(a) \equiv 2 \pmod{a^2 + 2}$ Since $3|a^2 + 2$, therefore $Q_k(a) \equiv 2 \pmod 3$ Hence

$$(6X_1^2 / Q_k(a)) = -(Q_k(a) / 3) = -(2 / 3)$$

$$= 1$$

$$= (-(a^4 + 4a^2 + 3) / Q_k(a))$$

Let $a^4 + 4a^2 + 3 = 2^m.c$ where c is odd. Then

$$1 = -(2^m.c / Q_k(a)) = -(Q_k(a) / c)$$

$$= -(-(a^4 + 4a^2 + 2) / c)$$

$$= -(1 / c) \text{ since } c \mid (a^4 + 4a^2 + 3)$$

$$= -1$$

which is clearly impossible. Thus $Q_{3r'\rho}(a) \neq 2NX^2$.

(iii) Suppose finally that $2|\rho$, $3\nmid r$. Then since $3|r\rho$, $3|\rho$. From (1.8), (1.9) and (1.11) therefore,

$$Q_{r\rho}(a) = Q_{\frac{1}{3}r\rho}(a)\,(Q_{\frac{1}{3}r\rho}(a)^2 - 3)$$

for all integers r. In particular, $Q_{\rho}(a) = Q_{\frac{1}{3}\rho}(a)\,(Q_{\frac{1}{3}\rho}(a)^3 - 3)$ Let $N = N_1N_2$ where $N_1 \mid Q_{\frac{1}{3}\rho}(a)$ and $N_2 \mid Q_{\frac{1}{3}\rho}(a)^2 - 3$ and if $3 \mid N$, let $3 \mid N_2$. Then as in the proof of theorem 1.16(c) we can show that $N_1 \mid Q_{\frac{1}{3}r\rho}(a)$, $N_2 \mid (Q_{\frac{1}{3}r\rho}(a)^2 - 3)$, and that if $3 \mid Q_{\frac{1}{3}r\rho}(a)$, $3 \mid Q_{\frac{1}{3}\rho}(a)$. If $3 \nmid \frac{1}{3}r\rho$, from (1.12) we see that we require either

$$Q_{\frac{1}{3}r\rho}(a) = 3N_1X_1^2$$

where $3N_1 \mid Q_{\frac{1}{3}\rho}(a)$, or

$$Q_{\frac{1}{3}r\rho}(a) = N_1X_1^2$$

where $N_1 \mid Q_{\frac{1}{3}\rho}(a)$. From theorem 1.16 (b) and theorem 1.1 again there are no solutions other than $r = \pm 1$.

If $3 \mid \frac{1}{3}r\rho$, we proceed as above until all the factors of 3 in ρ are exhausted and again see that $r = \pm 1$ gives the only solutions. This completes the proof of theorem 1.17.

THEOREM 1.18. Let N_1 be a positive odd square-free integer such that the rank of apparition of N_1, ρ_1, with respect to the sequence $Q_n(a)$ is defined; and let N_2 be a positive odd square-free integer such that $(N_2, Q_n(a)) = 1$ for all integers n. Let the rank of apparition of N_2 with respect to the sequence $P_n(a)$ be ρ_2. Then ρ_2 is odd and:

(a) $P_n(a) = N_1Y^2$ can occur only if $(n = 0)$, $(a = N_1Y^2, n = 2)$ or $(a = Y_1^2, a^2 + 2 = N_1Y_2^2, n = 4)$.

(b) $P_n(a) = 2N_1Y^2$ can occur only if $(n = 0)$, $(a = 1, N_1 = 161, \rho_1 = 6, n = 24)$ or $(a^2 + 1 = 2Y_1^2, a^3 + 3a = N_1Y_2^2, n = 6)$.

(c) $P_n(a) = N_2Y^2$ can occur only if $(n = 0)$ or $(n = \pm\rho_2, 3 \nmid \rho_2)$.

(d) $P_n(a) = 2N_2Y^2$ can occur only if ($n = 0$), ($a = 3$, $N_2 = 5$, $\rho_2 = 3$, $n = 6$) or ($n = \pm \rho_2$, $3 \mid \rho_2$).

Proof. We show first that ρ_2 is odd. For suppose by way of contradiction that $\rho_2 = 2\rho$. Then from (1.8)

$$P_{\rho_2}(a) = P_{\rho}(a)\ Q_{\rho}(a)$$

where $(N_2, Q_{\rho}(a)) = 1$. Since $N_2 \mid P_{\rho_2}(a)$, therefore $N_2 \mid P_{\rho}(a)$. But $\rho < \rho_2$, which contradicts the definition of ρ_2. Thus ρ_2 is odd.

(a) Suppose that $P_n(a) = N_1Y^2$. Now $N_1 \mid Q_{\rho_1}(a)$ and, therefore, $N_1 \mid (Q_{\rho_1}(a), P_n(a))$ where $N_1 > 2$. Thus from lemma 1.6 $N_1 \mid Q_{(n,\rho_1)}(a)$ and $\frac{n}{(n,\rho_1)}$ is an even integer. But since ρ_1 is the rank of apparition of N_1, clearly $(n,\rho_1) \geq \rho_1$, i.e. $(n,\rho_1) = \rho_1$. Thus $n = 2r\rho_1$, for some integer r. From (1.8) therefore, if $P_n(a) = N_1Y^2$,

$$N_1Y^2 = P_{2r\rho_1}(a) = P_{r\rho_1}(a)\ Q_{r\rho_1}(a)$$

where from (1.13), $(P_{r\rho_1}(a), Q_{r\rho_1}(a) = 1$ or 2.

If r is odd, from lemma 1.2, $N_1 \mid Q_{r\rho_1}(a)$ and so we require either

$$P_{r\rho_1}(a) = Y_1^2,\ Q_{r\rho_1}(a) = N_1Y_2^2$$

or

$$P_{r\rho_1}(a) = 2Y_1^2,\ Q_{r\rho_1}(a) = 2N_1Y_2^2$$

From theorems 1.3 and 1.4 the only solutions are

$r\rho_1 = 1$, $Y_1 = 1$, $Q_1(a) = a = N_1Y_2^2$;

$r\rho_1 = 2$, $a =$ a perfect square, $Y_1 = a^{\frac{1}{2}}$, $Q_2(a) = a^2 + 2 = N_1Y_2^2$.

If r is even, from lemma 1.1 and (1.8), $P_{\rho_1}(a)\ Q_{\rho_1}(a) = P_{2\rho_1}(a) \mid P_{r\rho_1}(a)$ and so $N_1 \mid P_{r\rho_1}(a)$. Thus we require either

$$P_{r\rho_1}(a) = N_1Y_1^2,\ Q_{r\rho_1}(a) = Y_2^2$$

or

$$P_{r\rho_1}(a) = 2N_1Y_1^2,\ Q_{r\rho_1}(a) = 2Y_2^2.$$

From theorems 1.1 and 1.2 the only solution, since r is even, is $r\rho_1 = 0$, $Y_1 = 0$, $Q_o(a) = 2 = 2Y_2^2$.

This completes the proof of (a).

(b) Suppose $P_n(a) = 2N_1Y^2$. As in (a) we can show that $n = 2r\rho_1$, for some integer r. Then from (1.8), if $P_n(a) = 2N_1Y^2$,

$$2N_1Y^2 = P_{r\rho_1}(a)\, Q_{r\rho_1}(a)$$

where, from (1.13), $(P_{r\rho_1}(a), Q_{r\rho_1}(a)) = 1$ or 2.
If r is odd, from lemma 1.2 again $N_1 \mid Q_{r\rho_1}(a)$ and so we require either

$$P_{r\rho_1}(a) = Y_1^2, \quad Q_{r\rho_1}(a) = 2N_1Y_2^2$$

or

$$P_{r\rho_1}(a) = 2Y_1^2, \quad Q_{r\rho_1}(a) = N_1Y_2^2$$

From theorems 1.3 and 1.4 the only solutions are

$r\rho_1 = 12$, $a = 1$, $Y_1 = 12$, $N_1 = 161$, $Y_2 = 1$;
$r\rho_1 = 3$, $P_3(a) = a^2 + 1 = 2Y_1^2$, $Q_3(a) = a^3 + 3a = N_1Y_2^2$.
If r is even, as in (a) $N_1 \mid P_{r\rho_1}(a)$ and so we require either

$$P_{r\rho_1}(a) = N_1Y_1^2, \quad Q_{r\rho_1}(a) = 2Y_2^2$$

or

$$P_{r\rho_1}(a) = 2N_1Y_1^2, \quad Q_{r\rho_1}(a) = Y_2^2$$

From theorems 1.1 and 1.2, since r is even, the only solution is $r\rho_1 = 0$, $Y_1 = 0$, $Q_o(a) = 2 = 2Y_2^2$.
This completes the proof of (b).

(c) Suppose that $P_n(a) = N_2Y^2$. Then from lemma 1.7 clearly $n = r\rho_2$, for some integer r.

(i) Suppose first that $r = 2r'$. Then if $P_n(a) = N_2 Y^2$, from (1.8)

$$N_2 Y^2 = P_{r'\rho_2}(a)\, Q_{r'\rho_2}(a)$$

where $N_2 \mid P_{r'\rho_2}(a)$ from lemma 1.7. Also, from (1.13), $(P_{r'\rho_2}(a), Q_{r'\rho_2}(a)) = 1$ or 2 so we require

$$Q_{r'\rho_2}(a) = X^2 \text{ or } 2X^2.$$

From theorems 1.1 and 1.2, since $N_2 > 2$, we see that the only solution is $r'\rho_2 = 0$.

(ii) Suppose now that $2 \nmid r\rho_2$, $3 \nmid r\rho_2$. Then if $P_{\rho_2}(a) = N_2 Y^2$ by theorem 1.15 and (1.6) $P_{r\rho_2}(a) \neq N_2 Y^2$ for any $r \neq \pm 1$, since N_2 is odd. If $P_{\rho_2}(a) \neq N_2 Y^2$ then $P_{\rho_2}(a) = N_2 . R Y_1^2$ for some square-free integer $R, R > 1$. Since $3 \nmid r\rho_2$, from (1.12) R is odd. But since $2 \nmid r\rho_2$, from (1.32)

$$P_{r\rho_2}(a) = P_{\rho_2}(a)\; P_r\left(Q_{\rho_2}(a)\right)$$

and thus, if $P_{r\rho_2}(a) = N_2 Y^2$,

$$P_r\left(Q_{\rho_2}(a)\right) = Rx^2$$

where from (1.11) $R \mid Q_{\rho_2}(a)^2 + 4$. Since $Q_{\rho_2}(a)$ is odd, from theorem 1.13 the only possibility is $r = \pm 5$, $R = \pm 5$, $Q_{\rho_2}(a) = 1$. But then $\rho_2 = 1$, $a = 1$ and $N_2 \mid P_1(1) = 1$ which is impossible. Thus if $P_{r\rho_2}(a) = N_2 Y^2$ in this case $r = \pm 1$.

(iii) Suppose finally that $2 \nmid r\rho_2$, $3 \mid r\rho_2$. Then from (1.14) and the first twelve values of $P_n(a)$, $P_{r\rho_2}(a) \equiv 2 \pmod 4$. Thus $P_{r\rho_2}(a) \neq N_2 Y^2$, where N_2 is odd. In particular $3 \nmid \rho_2$. This completes the proof of (c).

(d) Suppose that $P_n(a) = 2N_2Y^2$. Then again it is clear that from lemma 1.7 $n = r\rho_2$, for some integer r.

(i) Suppose first that $r = 2r'$. Then as in (c) we find we require

$$Q_{r'\rho_2}(a) = X^2 \text{ or } 2X^2.$$

From theorems 1.1 and 1.2, since $N_2 > 2$, we see that the only solutions are:

$r'\rho_2 = 0$, $P_0(a) = N_2 \cdot 0^2$, $Q_0(a) = 2 = 2X^2$;

$r'\rho_2 = 3$, $a = 3$, $N_2 = 5$, $Q_3(3) = 6^2$.

(ii) Suppose now that $2\nmid r$, $3 \mid r$. Let $r = 3t$. Then from (1.8), (1.9) and (1.11), if $P_n(a) = 2N_2Y^2$, we have

$$2N_2Y^2 = P_{t\rho_2}(a) \quad (Q_{t\rho_2}(a)^2 + 1)$$

since $2\nmid r\rho_2$. Also, by lemma 1.7 $N_2 \mid P_{t\rho_2}(a)$. From (1.11) $(P_{t\rho_2}(a), Q_{t\rho_2}(a)^2 + 1) = 1$ or 3, but since $3\nmid Q_{t\rho_2}(a)^2 + 1$, therefore $(P_{t\rho_2}(a), Q_{t\rho_2}(a)^2 + 1) = 1$. Thus we require either

$$Q_{t\ 2}(a) + 1 = Y_1^2$$

which is impossible since $|Q_{t\rho_2}(a)| > 0$, or

$$Q_{t\rho_2}(a)^2 + 1 = 2Y_1^2$$

From (1.12) this case requires $3\nmid t\rho_2$. Also $2\nmid t\rho_2$. From (1.31) therefore $t\rho_2 = \pm 1$. But this requires $N_2 \mid P_1(a) = 1$, which is impossible.

Thus $3\nmid r$.

(iii) Suppose finally that $2\nmid r$, $3\nmid r$. Then if $P_{r\rho_2}(a) = 2N_2Y^2$, from (1.12) $3 \mid \rho_2$. From (1.8), (1.9) and (1.11) then we find

$$2N_2Y^2 = P_{\frac{1}{3}r\rho_2}(a)\,(Q_{\frac{1}{3}r\rho_2}(a)^2 + 1)$$

where $(P_{\frac{1}{3}r\rho_2}(a),\ Q_{\frac{1}{3}r\rho_2}(a)^2 + 1) = 1$. Let $N_2 = N_3N_4$ where $N_3 \mid P_{\frac{1}{3}\rho_2}(a)$, $N_4 \mid Q_{\frac{1}{3}\rho_2}(a)^2 + 1$. Since $3\nmid r$, from lemma 1.4 $(P_{\frac{1}{3}r\rho_2}(a),\ P_{\rho_2}(a)) = P_{\frac{1}{3}\rho_2}(a)$ and so $N_3 \mid P_{\frac{1}{3}r\rho_2}(a)$, $N_4 \mid Q_{\frac{1}{3}r\rho_2}(a)^2 + 1$. Thus we require either

$$P_{\frac{1}{3}r\rho_2}(a) = N_3Y_1^2$$

or

$$P_{\frac{1}{3}r\rho_2}(a) = 2N_3Y_1^2$$

If $N_3 = 1$, from theorems 1.3 and 1.4 since $2\nmid r$, $3\nmid r$, $r = \pm 1$.
If $N_3 > 1$, from (c) the first possibility requires $r = \pm 1$.
The second possibility, from (1.12) requires $3 \mid \frac{1}{3}r\rho_2$. We therefore repeat the above process until all the factors of 3 in ρ_2 are exhausted when again we see that the only possibility is $r = \pm 1$.

This completes the proof of the theorem.

THEOREM 1.19. Let N be a positive odd square-free integer such that $N \nmid Q_r(a)$ for any integer r, but $(N, Q_s(a)) > 2$ for at least one integer s. Let the rank of apparition of N with respect to the sequence $P_n(a)$ be ρ. Then

(a) $P_n(a) = NY^2$ can occur only if $(n = 0)$, $(a = 5,\ N = 455,\ \rho = 6,\ n = 12)$ or $(n = \rho)$.

(b) $P_n(a) = 2NY^2$ can occur only if $(n = 0)$ or $(n = \rho)$.

Proof. If $P_n(a) = NY^2$ or $2NY^2$ where $(N, Q_s(a)) > 2$, from lemma 1.6 we see that n must be even. If $n = 0$, $P_0(a) = N.0^2 = 2N.0^2$. If $n \neq 0$, put $n = 2^t.c$ where c is odd, $t \geq 1$. Then from (1.8) we find

$$P_n(a) = P_c(a)\,Q_c(a)\,Q_{2c}(a) \cdots\cdots Q_2^{t-1}{}_c(a)$$

where, from lemmas 1.3 and 1.6,

$$(P_c(a), Q_{2^{i_c}}(a)) \mid 4, \quad (Q_{2^{i_c}}(a), Q_{2^{j_c}}(a)) \mid 2 \text{ where } i \neq j.$$

Since $N \mid P_n(a)$, let

$$N = N_o N_1 N_2 \ldots N_{t-1}$$

where

$$N_o \mid P_c(a), \quad N_i \mid Q_{2^{i_c}}(a): 1 \leq i \leq t-1.$$

Now we see that if $P_n(a) = NY^2$ or $2NY^2$, then we require

$$P_c(a) = N_o Y_o^2 \text{ or } 2N_o Y_o^2$$

and

$$Q_{2^{i_c}}(a) = N_i Y_i^2 \text{ or } 2N_i Y_i^2.$$

If $N_{t-1} = 1$, from theorems 1.1 and 1.2 we find that the only solution of $P_n(a) = NY^2$ is $P_{12_2}(5) = 455.396^2$, and that there are no solutions of $P_n(a) = 2NY^2$.

If $N_{t-1} > 1$, from lemma 1.8 we see that the rank of apparition of N_{t-1} with respect to the sequence $Q_n(a)$ is of the form $2^{t-1}\sigma$, where σ is odd. Thus, from lemma 1.6 $\rho = 2^t.c'$ where $\sigma \mid c'$.

From lemma 1.7 now $c' \mid c$. Since we require $Q_{2^{t-1}_c}(a) = N_{t-1}Y_{t-1}^2$ or $2N_{t-1}Y_{t-1}^2$, therefore, from theorems 1.16 and 1.17 we must have $\sigma = c' = c$.

This completes the proof of theorem 1.19 and concludes this chapter.

CHAPTER 2.

In this chapter we suppose that the equation $X^2 - dY^2 = -4$ has solutions, but only even ones.

As in chapter 1 we seek solutions of the equations $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$ among the solutions of $X^2 - dY^2 = \pm 1, \pm 4$ but the method gives only very limited results in this case.

We begin by establishing some results concerning the solutions of the equations $X^2 - dY^2 = \pm 1, \pm 4$ which are very similar to those obtained in the first chapter.

Since all the solutions of $X^2 - dY^2 = -4$ are being supposed even, if $X = A, Y = B$ is the fundamental solution clearly A and B are both even. We put $A = 2a$, $B = 2b$. Then again, as in (6), the general solution of $X^2 - dY^2 = -4$ is given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{2a + 2bd^{\frac{1}{2}}}{2}\right)^{2n-1}$$

$$= 2\,(a + bd^{\frac{1}{2}})^{2n-1}$$

As before we write $\alpha = a + bd^{\frac{1}{2}}$, $\beta = a - bd^{\frac{1}{2}}$ and have immediately

$$\alpha + \beta = 2a; \quad \alpha\beta = -1 \tag{2.1}$$

Again we define for all integers n,

$$P_n(2a) = \frac{1}{2bd^{\frac{1}{2}}}(\alpha^n - \beta^n) \tag{2.2}$$

$$Q_n(2a) = \alpha^n + \beta^n \tag{2.3}$$

and obtain exactly as before

$$P_{n+2}(2a) = 2aP_{n+1}(2a) + P_n(2a) \tag{2.4}$$

$$Q_{n+2}(2a) = 2aQ_{n+1}(2a) + Q_n(2a) \tag{2.5}$$

$$P_{-n}(2a) = (-1)^{n-1} P_n(2a) \tag{2.6}$$

$$Q_{-n}(2a) = (-1)^n Q_n(2a) \tag{2.7}$$

Also, $P_0(2a) = 0, P_1(2a) = 1$, $Q_0(2a) = 2$ and $Q_1(2a) = 2a$. Thus it is clear that $P_n(2a)$ and $Q_n(2a)$ are integers for all integers n, and moreover positive for positive n. The first few values are:

n	$P_n(2a)$	$Q_n(2a)$
0	0	2
1	1	2a
2	2a	$4a^2 + 2$
3	$4a^2 + 1$	$8a^3 + 6a$
4	$8a^3 + 4a$	$16a^4 + 16a^2 + 2$
5	$16a^4 + 12a^2 + 1$	$32a^5 + 40a^3 + 10a$
6	$32a^5 + 32a^3 + 6a$	$64a^6 + 96a^4 + 36a^2 + 2$

Again as in chapter 1 we obtain

$$2P_{m+n}(2a) = P_m(2a)Q_n(2a) + P_n(2a)Q_m(2a) \tag{2.8}$$

$$2Q_{m+n}(2a) = (4a^2+4)P_m(2a)P_n(2a) + Q_m(2a)Q_n(2a) \tag{2.9}$$

$$Q_n(2a) = Q_{2n}(2a) + (-1)^n.2 \tag{2.10}$$

$$Q_n(2a)^2 = (4a^2+4)P_n(2a)^2 + (-1)^n.4 \tag{2.11}$$

Now from(2.9) we find

$$\begin{aligned} 2Q_{m+\varepsilon N}(2a) &= (4a^2+4)P_m(2a)P_{2N}(2a) + Q_m(2a)Q_{2N}(2a) \\ &= (4a^2+4)P_m(2a)P_N(2a)Q_N(2a) + Q_m(2a)\big(Q_N(2a)^2 + \\ &\qquad (-1)^{N-1}.2\big) \end{aligned}$$

from (2.8) and (2.10)

$$\equiv (-1)^{N-1}.2\, Q_m(2a) \pmod{2Q_N(2a)}$$

for clearly, since $Q_n(2a) = (a + bd^{\frac{1}{2}})^n + (a - bd^{\frac{1}{2}})^n$ where a and b are integers, $Q_n(2a)$ is even for all integers n. Thus

$$Q_{m+2N}(2a) \equiv (-1)^{N-1} Q_m(2a) \pmod{Q_N(2a)} \qquad (2.12)$$

and similarly

$$Q_{m+2N}(2a) \equiv (-1)^N Q_m(2a) \pmod{(4a^2 + 4)P_N(2a)} \qquad (2.13)$$

Now if a is odd, clearly $Q_o(2a) \equiv 2 \pmod 4$ and $Q_1(2a) \equiv 2 \pmod 4$. Suppose that a is odd and $Q_r(2a) \equiv 2 \pmod 4$ for all $r \leq n$. Then from (2.5)

$$Q_{n+1}(2a) = 2a\, Q_n(2a) + Q_{n-1}(2a)$$

where $4 \mid 2aQ_n(2a)$ and hence

$$Q_{n+1}(2a) \equiv Q_{n-1}(2a) \equiv 2 \pmod 4$$

by the inductive hypothesis. Thus we have

$$\text{if a is odd, then } Q_n(2a) \equiv 2 \pmod 4 \qquad (2.14)$$

From (2.8) $P_{2n}(2a) = P_n(2a)\, Q_n(2a)$ and therefore, from (2.14), $P_{2n}(2a)$ is even. Clearly $P_1(2a) \equiv 1 \pmod 4$. Suppose that $P_{2m+1}(2a) \equiv 1 \pmod 4$ for all $2m+1 \leq 2n-1$. Then from (2.4)

$$P_{2n+1}(2a) = 2a\, P_{2n}(2a) + P_{2n-1}(2a)$$

and hence

$$P_{2n+1}(2a) \equiv P_{2n-1}(2a) \equiv 1 \pmod 4$$

i.e.

$$2 \mid P_{2n}(2a);\quad P_{2n+1}(2a) \equiv 1 \pmod 4 \qquad (2.15)$$

From (2.13) we find

$$Q_{m+4}(2a) \equiv Q_m(2a) \pmod{(4a^2+4)P_2(2a)}$$

and if a is odd, $8 \mid 4a^2 + 4$ and $2 \mid P_2(2a)$. Thus we have

$$Q_{m+4}(2a) \equiv Q_m(2a) \pmod{16}$$

i.e.

$$\text{if a is odd, then } \tfrac{1}{2}Q_{m+4}(2a) \equiv \tfrac{1}{2}Q_m(2a) \pmod 8 \qquad (2.16)$$

It will be readily seen that the proofs of lemmas 1.1 - 1.6 do not depend in any essential way upon the fact that a is odd, and the results carry over to $Q_n(2a)$ and $P_n(2a)$. We need only one of these results, which for the sake of completeness we prove here.

LEMMA 2.1. $Q_n(2a) \mid Q_{nt}(2a)$ for all odd integers t.

Proof. From (2.7) we see that we need only consider $t \geqslant 0$. Hence we use proof by induction. The result is clearly true for $t = 1$. Assume it true for $t = 2r-1$. Then from (2.9)

$$2Q_{(2r+1)n}(2a) = (4a^2+4)P_{(2r-1)n}(2a)P_{2n}(2a) + Q_{(2r-1)n}(2a).Q_{2n}(2a)$$

$$= (4a^2+4)P_{(2r-1)n}(2a)P_n(2a)Q_n(2a) + Q_{(2r-1)n}(2a)Q_{2n}(2a)$$

from(2.8). By the inductive hypothesis and (2.14) clearly $2Q_n(2a)$ divides the R.H.S. of the above equation and hence the result by induction.

Finally we observe that if $2\alpha = 2a + 2bd^{\frac{1}{2}}$ is the fundamental solution of the equation $X^2 - dY^2 = -4$, then the fundamental solutions of the equations $X^2 - dY^2 = 4$; $X^2 - dY^2 = -1$ and $X^2 - dY^2 = 1$ are respectively $2\alpha^2$, α, and α^2. Hence

the general solution of $X^2 - dY^2 = -4$ is $X = Q_{2n-1}(2a)$,

$$Y = 2bP_{2n-1}(2a) \qquad \text{(II.I)}$$

the general solution of $X^2 - dY^2 = 4$ is $X = Q_{2n}(2a)$,

$$Y = 2bP_{2n}(2a) \qquad \text{(II.II)}$$

the general solution of $X^2 - dY^2 = -1$ is $X = \frac{1}{2}Q_{2n-1}(2a)$,

$$Y = bP_{2n-1}(2a) \qquad \text{(II.III)}$$

the general solution of $X^2 - dY^2 = 1$ is $X = \frac{1}{2}Q_{2n}(2a)$,

$$Y = bP_{2n}(2a) \qquad \text{(II.IV)}$$

We are seeking solutions of $X^4 - dY^2 = \pm 1, \pm 4$ and $X^2 - dY^4 = \pm 1, \pm 4$. Clearly the solutions of $X^2 - dY^4 = -4$ are given by $X = Q_{2n-1}(2a)$, $Y^2 = 2bP_{2n-1}(2a)$ with similar results for the other equations. We would therefore like to prove results which would enable us to say when $P_n(2a) = Y^2, 2Y^2$ and $Q_n(2a) = X^2, 2X^2$. We note that from (2.14) clearly there are no solutions of $Q_n(2a) = X^2$ if a is odd. It is not, however, possible to give results covering all the above equations even when we restrict a to being odd. The results which have been obtained are contained in the following two theorems.

THEOREM 2.1. The equation $Q_{2n}(2a) = 2X^2$ has only the solution $n = 0$ if a is odd.

Proof. (i). If $2n \equiv 2 \pmod 4$ then $Q_{2n}(2a) \neq 2X^2$. For, by repeated application of (2.16)

$$\tfrac{1}{2}Q_{2n}(2a) \equiv \tfrac{1}{2}Q_2(2a) = \tfrac{1}{2}(4a^2 + 2) \equiv 3 \pmod 4$$

and hence $\frac{1}{2}Q_{2n}(2a) \neq X^2$.

(ii) If $4 \mid 2n$ then $Q_{2n}(2a) \neq 2X^2$. For suppose first that $3 \nmid 2n$. Then $2n = 6m \pm 2$ where m is an odd integer. By (2.12)

$$Q_{2n}(2a) = Q_{6m\pm2}(2a) \equiv Q_{\pm2}(2a) \pmod{Q_{3m}(2a)}$$
$$\equiv 4a^2 + 2 \pmod{Q_{3m}(2a)} \text{ by (2.7)}$$

By lemma 2.1 $Q_3(2a) | Q_{3m}(2a)$ since m is odd.

$Q_3(2a) = 2a(4a^2 + 3)$ and so

$$(2Q_{2n}(2a)/4a^2 + 3) = (2(4a^2 + 2) / 4a^2 + 3)$$
$$= (-2 / 4a^2 + 3)$$
$$= -1 \text{ since a is odd.}$$

Thus $2Q_{2n}(2a) \neq 4X^2$.

If $3 | 2n$, from (2.8) - (2.11), putting $2n = 6m$,

$$2Q_{2n}(2a) = 2Q_{2m}(2a)\,(Q_{2m}(2a)^2 - 3)$$

where $(Q_{2m}(2a), Q_{2m}(2a)^2 - 3) = 1$ or 3. Thus if $Q_{2n}(2a) = 2X^2$, we require either

$$Q_{2m}(2a)^2 - 3 = X_1^2$$

which implies $n = 0$, or

$$Q_{2m}(2a)^2 - 3 = 3X_1^2$$

which is impossible modulo 9.

This completes the proof.

THEOREM 2.2. The equation $P_{2n}(2a) = Y^2$ has only the solution $n = 0$ if a is odd.

Proof. From (2.8) we find

$$P_{2n}(2a) = P_n(2a)\, Q_n(2a)$$

where clearly, from (2.11), $(P_n(2a), Q_n(2a)) = 1$ or 2. Thus if $P_{2n}(2a) = Y^2$ we require either

$$P_n(2a) = Y_1^2 \; ; \; Q_n(2a) = Y_2^2$$

which from (2.14) is impossible, or

$$P_n(2a) = 2Y_1^2 \quad ; \quad Q_n(2a) = 2Y_2^2.$$

From theorem 2.1 the second equation requires n odd or n =0. If n is odd, from (2.15) P_n (2a) is also odd and so $P_n(2a) \neq 2Y^2$. Hence the only solution is n = 0.

This completes the proof.

These are the only results we have been able to obtain in this case.

CHAPTER 3.

In this chapter we suppose that the equation $X^2 - dY^2 = -4$ has no solutions but that the equation $X^2 - dY^2 = 4$ has odd solutions, i.e. solutions (X,Y) where X and Y are both odd.

The results at the beginning of this section, up to and including theorem 3.4 are due to J.H.E.Cohn and are taken from (4).

We seek solutions of the equations $X^4 - dY^2 = 1,4$; $X^2 - dY^4 = 1,4$; $X^2 - dN^2Y^4 = 1,4$ and $N^2X^4 - dY^2 = 1,4$ among the solutions of $X^2 - dY^2 = 1,4$.

We begin by establishing some results concerning the solutions of the equations $X^2 - dY^2 = 1,4$ which are very similar to those set up at the beginning of chapter 1 for the equations $X^2 - dY^2 = \pm 1, \pm 4$ in the case where the equation $X^2 - dY^2 = -4$ had odd solutions.

Since $X^2 - dY^2 = 4$ has odd solutions clearly $d \equiv 5 \pmod 8$. If $X = a$, $Y = b$ is the fundamental solution it is well-known that the general solution of $X^2 - dY^2 = 4$ is given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{a + bd^{\frac{1}{2}}}{2}\right)^n$$

See for example (6).

Hence, since we are assuming that there is a solution for which X and Y are both odd, a and b will be both odd. We write as before $\alpha = \frac{1}{2}(a + bd^{\frac{1}{2}})$, $\beta = \frac{1}{2}(a - bd^{\frac{1}{2}})$ and have immediately

$$\alpha + \beta = a \; ; \; \alpha\beta = 1 \qquad (3.1)$$

We now define, for all integers n,

$$p_n(a) = \frac{1}{bd^{\frac{1}{2}}}\left(\alpha^n - \beta^n\right) \qquad (3.2)$$

$$q_n(a) = \alpha^n + \beta^n \tag{3.3}$$

Then

$$p_{n+2}(a) = \frac{1}{bd^2}(\alpha^{n+2} - \beta^{n+2})$$

$$= \frac{1}{bd^2}(\alpha^{n+1} - \beta^{n+1})(\alpha+\beta) + \frac{1}{bd^2}\alpha\beta(\beta^n - \alpha^n)$$

i.e.

$$p_{n+2}(a) = ap_{n+1}(a) - p_n(a) \tag{3.4}$$

from (3.1) and (3.2). Similarly, from (3.1) - (3.3) we find

$$q_{n+2}(a) = aq_{n+1}(a) - q_n(a) \tag{3.5}$$

$$p_{-n}(a) = -p_n(a) \tag{3.6}$$

$$q_{-n}(a) = q_n(a) \tag{3.7}$$

Also $p_0(a) = 0, p_1(a) = 1, q_0(a) = 2$ and $q_1(a) = a$ and thus it is clear that $p_n(a)$ and $q_n(a)$ are integers for all integers n and moreover positive for positive n. The first few values are:

n	$p_n(a)$	$q_n(a)$
0	0	2
1	1	a
2	a	$a^2 - 2$
3	$a^2 - 1$	$a^3 - 3a$
4	$a^3 - 2a$	$a^4 - 4a^2 + 2$
5	$a^4 - 3a^2 + 1$	$a^5 - 5a^3 + 5a$
6	$a^5 - 4a^3 + 3a$	$a^6 - 6a^4 + 9a^2 - 2$

We also observe that since the equation $X^2 - dY^2 = -4$ has solutions for $d = 5$ and $d = 13$ in the case that we are considering $d \geq 21$. Now $a^2 = db^2 + 4$ and therefore

$$a \geq 5 \tag{3.8}$$

Now from (3.2)

$$2p_{m+n}(a) = \frac{2}{bd^{\frac{1}{2}}} (\alpha^{m+n} - \beta^{m+n})$$

$$= \frac{1}{bd^{\frac{1}{2}}} (\alpha^{m} - \beta^{m}) (\alpha^{n} + \beta^{n})$$

$$+ \frac{1}{bd^{\frac{1}{2}}} (\alpha^{n} - \beta^{n}) (\alpha^{m} + \beta^{m})$$

$$= p_m(a)\, q_n(a) + p_n(a)\, q_m(a)$$

from (3.2) and (3.3), i.e.

$$2p_{m+n}(a) = p_m(a)\, q_n(a) + p_n(a)\, q_m(a) \tag{3.9}$$

Similarly, from (3.1) - (3.3) we have

$$2q_{m+n}(a) = (a^2 - 4)\, p_m(a)\, p_n(a) + q_n(a)\, q_m(a) \tag{3.10}$$

$$q_n(a)^2 = q_{2n}(a) + 2 \tag{3.11}$$

$$q_n(a)^2 = (a^2 - 4)\, p_n(a)^2 + 4 \tag{3.12}$$

Now from (3.12) obviously $2 \mid q_n(a) \Leftrightarrow 2 \mid p_n(a)$. Also, from (3.1) and (3.2)

$$p_{3n}(a) = \frac{1}{bd^{\frac{1}{2}}} (\alpha^{3n} - \beta^{3n})$$

$$= \frac{1}{bd^{\frac{1}{2}}} (\alpha^{n} - \beta^{n}) ((\alpha^{n} + \beta^{n})^2 - 1)$$

$$= p_n(a) (q_n(a)^2 - 1)$$

Thus, since $2 \mid p_n(a) \Leftrightarrow 2 \mid q_n(a)$, $2 \mid p_{3n}(a)$. From (3.4)

$$p_{3n}(a) = a p_{3n-1}(a) - p_{3n-2}(a)$$

where a is odd and therefore $p_{3n-1}(a)$ and $p_{3n-2}(a)$ have the same parity. If they are both even $p_n(a)$ is even for all n which we are assuming not to be the case. Hence they are both odd. This gives us

$$2 \mid p_n(a) \Leftrightarrow 2 \mid q_n(a) \Leftrightarrow 3 \mid n \tag{3.13}$$

(3.12) and (3.13) now give

$$(p_n(a),\ q_n(a)\ ) = 1 \text{ if } 3\nmid n\ ;\quad (p_n(a), q_n(a)\ ) = 2 \text{ if } 3 \mid n \qquad (3.14)$$

From (3.9) we find

$$\begin{aligned} 2p_{n+6}(a) &= p_n(a)q_6(a) + q_n(a)p_6(a) \\ &= p_n(a)(q_3(a)^2 - 2) + q_n(a)p_3(a)q_3(a) \text{ from (3.9)} \end{aligned}$$

and (3.11)

i.e.

$$2p_{n+6}(a) = p_n(a)\left((a^2 - 4)p_3(a)^2 + 2\right) + q_n(a)p_3(a)q_3(a)$$

from (3.12)

$$\equiv 2p_n(a) \pmod{2p_3(a)}$$

since $2 \mid p_3(a)$ and $2 \mid q_3(a)$. But $p_3(a) = a^2 - 1 \equiv 0 \pmod 8$ and therefore $2p_{n+6}(a) \equiv 2p_n(a) \pmod{16}$. By similar means we may prove all the following;

$$p_{n+6}(a) \equiv p_n(a) \pmod 8\ ;\ p_{n+12}(a) \equiv p_n(a) \pmod{16} \qquad (3.15)$$

$$q_{n+6}(a) \equiv q_n(a) \pmod 8\ ;\ q_{n+12}(a) \equiv q_n(a) \pmod{16} \qquad (3.16)$$

As in chapter 1 again we use k to denote an integer, not necessarily positive, which is even but not divisible by 3. From(3.11) clearly

$$q_k(a) \equiv 7 \pmod 8 \qquad (3.17)$$

Now from (3.9) and (3.11) we have

$$\begin{aligned} 2p_{m+2N}(a) &= p_m(a)\, q_{2N}(a) + q_m(a)p_{2N}(a) \\ &= p_m(a)(q_N(a)^2 - 2) + q_m(a)p_N(a)q_N(a) \\ &\equiv \begin{cases} -2p_m(a) \pmod{q_N(a)\ } \text{ if } 3\nmid N \\ -2p_m(a) \pmod{2q_N(a)\ } \text{ if } 3 \mid N \quad \text{from (3.13)} \end{cases} \end{aligned}$$

Thus, in either case, from (3.13)

$$p_{m+2N}(a) \equiv -p_m(a) \pmod{q_N(a)} \tag{3.18}$$

Similarly we find

$$q_{m+2N}(a) \equiv -q_m(a) \pmod{q_N(a)} \tag{3.19}$$

$$p_{m+2N}(a) \equiv p_m(a) \pmod{p_N(a)} \tag{3.20}$$

$$q_{m+2N}(a) \equiv q_m(a) \pmod{(a^2-4)p_N(a)} \tag{3.21}$$

From(3.17) together with (3.18) - (3.19) we then have

$$p_{m+2k}(a) \equiv -p_m(a) \pmod{q_k(a)} \tag{3.22}$$

$$q_{m+2k}(a) \equiv -q_m(a) \pmod{q_k(a)} \tag{3.23}$$

Taking N = 1 in (3.19) and (3.21) we have, by induction,

$$q_{2n}(a) \equiv (-1)^n.2 \pmod{a} \tag{3.24}$$

$$q_{2n}(a) \equiv 2 \pmod{a^2-4} \tag{3.25}$$

$$q_{2n+1}(a) \equiv a \pmod{a^2-4} \tag{3.26}$$

Also from(3.9)

$$\begin{aligned} 2p_{n+2}(a) &= p_n(a)(a^2-2) + q_n(a).a \\ &\equiv 2p_n(a) + aq_n(a) \pmod{a^2-4} \end{aligned}$$

and using this equation, (3.25) and (3.26) a simple inductive arguement will show that

$$p_{2n}(a) \equiv na \pmod{a^2-4} \tag{3.27}$$

$$p_{2n+1}(a) \equiv 2n+1 \pmod{a^2-4} \tag{3.28}$$

Thus, by (3.17) and (3.24), if $2|k$, $3\nmid k$, we have

$$(a \,/\, q_k(a)) = ((-1)^{\frac{1}{2}k+1} \cdot 2 \,/\, a) \qquad (3.29)$$

Now since $2 \mid k$, $3 \nmid k$, $k \equiv \pm 2 \pmod 6$ and so, from (3.19) and (3.7) we have

$$q_k(a) \equiv -q_{k-6}(a) \equiv \cdots \equiv \pm q_{\pm 2}(a) = \pm q_2(a) \pmod{q_3(a)}$$

i.e. $$q_k(a) \equiv \pm (a^2 - 2) \pmod{\tfrac{1}{2}(a^3 - 3a)}$$

Suppose now that $a \equiv 3 \pmod 8$. Then $\frac{1}{2}(a^3 - 3a) \equiv 1 \pmod 4$ and

$$\begin{aligned}(2q_3(a) \,/\, q_k(a)) &= (q_k(a) \,/\, \tfrac{1}{2}q_3(a)) = (a^2 - 2 \,/\, \tfrac{1}{2}(a^3 - 3a)) \\ &\text{since } \tfrac{1}{2}(a^3 - 3a) \equiv 1 \pmod 4 \\ &= (a^2 - 2 \,/\, a)(a^2 - 2 \,/\, \tfrac{1}{2}(a^2 - 3)) \\ &= (-2 \,/\, a)(1 \,/\, \tfrac{1}{2}(a^2 - 3)) \\ &= 1 \text{ since } a \equiv 3 \pmod 8;\end{aligned}$$

Thus

$$\text{if } a \equiv 3 \pmod 8 \text{ then } (2q_3(a) \,/\, q_k(a)) = 1 \qquad (3.30)$$

By similar means we can prove that

$$\text{if } 3 \nmid n \text{ then } (p_{3n}(a) \,/\, q_{kn}(a)) = (p_n(a) \,/\, q_{kn}(a)) \qquad (3.31)$$

Now let n be an integer such that $2 \nmid n$, $3 \nmid n$ and suppose that $q_n(a)^2 - 1 = 2y^2$. Then from (3.11) we have

$$q_{2n}(a) = 2y^2 - 1.$$

Let $n = \pm 1 + rk$ where r is odd and $k = 2^m$, $m \geqslant 2$. Then $k = 6t \pm 2$ where t is odd since $4 \nmid k$. Thus from (3.19) and (3.7)

$$q_k(a) \equiv -q_{k-6}(a) \equiv \cdots \equiv (-1)^t q_{\pm 2}(a) \equiv -q_2(a) \pmod{q_3(a)}$$

If $n \neq \pm 1$, repeated applications of (3.23) together with (3.7) now give

$$\begin{aligned}2y^2 - 1 = q_{2n}(a) \equiv (-1)^r q_{\pm 2}(a) &\equiv -q_2(a) \pmod{q_k(a)} \\ &\equiv -(a^2 - 2) \pmod{q_k(a)}\end{aligned}$$

i.e.

$$2y^2 \equiv -(a^2 - 3) \pmod{q_k(a)}$$

Hence

$$(2y^2 / q_k(a)) = (-1 / q_k(a)) (a^2 - 3 / q_k(a))$$

i.e.

$$\begin{aligned} 1 &= (q_k(a) / \tfrac{1}{2}(a^2 - 3)) \text{ by (3.17)} \\ &= (-(a^2 - 2) / \tfrac{1}{2}(a^2 - 3)) \\ &= -1 \text{ since } \tfrac{1}{2}(a^2 - 3) \equiv -1 \pmod 4 \end{aligned}$$

This is clearly impossible and thus

$$\text{if } 2\nmid n,\ 3\nmid n, \text{ then } q_n(a)^2 - 1 = 2y^2 \text{ implies that } n = \pm 1. \tag{3.32}$$

Now a simple inductive arguement, using (3.10), will show

$$\text{if } 3\nmid a, \text{ then } q_{2n}(a) \equiv 2 \pmod 3 \tag{3.33}$$

Suppose now that n is odd and $q_n(a)^2 - 1 = Ry^2$, where $R = 3$ or 6. Then from (3.11), $q_{2n}(a) = Ry^2 - 1$. Since n is odd, we may write $2n = \pm 2 + 2.3^r.k$ where $4\mid k$, $3\nmid k$. Thus if $n \neq \pm 1$, repeated applications of (3.23) give

$$\begin{aligned} Ry^2 - 1 &\equiv -q_{\pm 2}(a) \pmod{q_k(a)} \\ &\equiv -a^2 + 2 \pmod{q_k(a)} \end{aligned}$$

Since $4\mid k$, $3\nmid k$, from (3.19) and (3.13), $(q_k(a), q_3(a)) = 1$ and so

$$(Ry^2 / q_k(a)) = (-(a^2 - 3) / q_k(a))$$

i.e.

$$(3 / q_k(a)) = -(\tfrac{1}{2}(a^2 - 3) / q_k(a)) \text{ by (3.17)}$$

Since $\frac{1}{2}(a^2 - 3) \equiv -1 \pmod 4$, therefore

$$(q_k(a) / 3) = -(q_k(a) / \tfrac{1}{2}(a^2 - 3))$$

But $\frac{1}{2}(a^2 - 3) \mid q_3(a)$, and, since $4 \mid k$, $3 \nmid k$, we may write $k = \pm 2 + 6t$ where t is odd. Thus from (3.19)

$$q_k(a) \equiv -q_{k-6}(a) \equiv \cdots \equiv (-1)^t q_{\pm 2}(a) \pmod{q_3(a)}$$

and hence

$$\begin{aligned}(q_k(a) / 3) &= -(-(a^2 - 2) / \tfrac{1}{2}(a^2 - 3)) \\ &= 1 \text{ since } \tfrac{1}{2}(a^2 - 3) \equiv -1 \pmod 4\end{aligned}$$

Hence from (3.33) we see that

$$\begin{aligned}&\text{if } 3 \nmid a,\ 2 \nmid n,\ R = 3 \text{ or } 6,\ \text{then } q_n(a)^2 - 1 = Ry^2 \\ &\qquad \text{implies } n = \pm 1. \qquad (3.34)\end{aligned}$$

From (3.2) and (3.3)

$$\begin{aligned}\alpha^n &= \tfrac{1}{2} q_n(a) + bd^{\frac{1}{2}} p_n(a) \\ \beta^n &= \tfrac{1}{2} q_n(a) - bd^{\frac{1}{2}} p_n(a)\end{aligned}$$

whence

$$\begin{aligned}p_m\big(q_n(a)\big) &= \frac{1}{bp_n(a)d^{\frac{1}{2}}}(\alpha^{mn} - \beta^{mn}) \\ &= \frac{p_{mn}(a)}{p_n(a)}\end{aligned}$$

i.e.

$$p_{mn}(a) = p_n(a)\, p_m\big(q_n(a)\big) \qquad (3.35)$$

Similarly we find that

$$q_{mn}(a) = q_m\left(q_n(a)\right) \qquad (3.36)$$

Finally we observe that if $2\alpha = a + bd^{\frac{1}{2}}$ is the fundamental solution of $X^2 - dY^2 = 4$ and a and b are both odd, then α^3 is the fundamental solution of the equation $X^2 - dY^2 = 1$. Hence the general solution of $X^2 - dY^2 = 4$ is $X = q_n(a), Y = bp_n(a)$ (III.I), the general solution of $X^2 - dY^2 = 1$ is $X = \frac{1}{2}q_{3n}(a), Y = \frac{1}{2}bp_{3n}(a)$ (III.II

Now we are seeking solutions of the equations $X^4 - dY^2 = 1,4$; $X^2 - dY^4 = 1,4$; $N^2X^4 - dY^2 = 1,4$ and $X^2 - dN^2Y^4 = 1,4$. Clearly the solutions of $X^4 - dY^2 = 1$ are given by $X^2 = \frac{1}{2}q_{3n}(a)$, $Y = \frac{1}{2}bp_{3n}(a)$, with corresponding results for the other equations. We therefore wish to prove theorems which will enable us to say when $p_n(a) = Y^2, NY^2$ and $q_n(a) = X^2, NX^2$, where N is a square-free integer. We are able to deal with the equations $p_n(a) = Y^2, 2Y^2$ and $q_n(a) = X^2, 2X^2$ immediately. The results are contained in the following four theorems.

THEOREM 3.1. The equation $q_n(a) = X^2$ has

a) two solutions $n = \pm 1$ if a is a perfect square;

b) no solutions otherwise.

Proof. (i) If n is even, by (3.11)

$$q_n(a) = q_{\frac{1}{2}n}(a)^2 - 2 \neq X^2.$$

(ii) If $n \equiv 3 \pmod 6$, by (3.16)

$$q_n(a) \equiv q_3(a) = a^3 - 3a \equiv -2a \pmod 8$$

and thus, since a is odd, $q_n(a) \neq X^2$.

(iii) If $n \equiv \pm 1 \pmod 6$, by (3.16) and (3.7)

$$q_n(a) \equiv q_{\pm 1}(a) = a \pmod 8$$

and so $q_n(a) \neq X^2$ except possibly if $a \equiv 1 \pmod 8$.

(iv) If $a \equiv 1 \pmod 8$ and n is odd, then $q_n(a) \neq X^2$ except possibly for $n = \pm 1$. For if $n \neq \pm 1$ we may write $n = \pm 1 + 2.3^r.k$ where $2|k$, $3\nmid k$, and then repeated applications of (3.23) give

$$q_n(a) \equiv (-1)3^r \; q_1(a) \pmod{q_k(a)}$$

$$\equiv -a \pmod{q_k(a)} \text{ by (3.7)}$$

Thus

$$(q_n(a) \,/\, q_k(a)) = (-a \,/\, q_k(a)) = -(a \,/ q_k)(a)) \text{ by (3.17)}$$

$$= -(2 \,/\, a) \text{ by (3.29)}$$

$$= -1 \text{ since } a \equiv 1 \pmod 8.$$

Thus $q_n(a) \neq X^2$ except possibly if $n = \pm 1$ and since $q_{\pm 1}(a) = a$, this occurs if and only if a is a perfect square.

This completes the proof.

THEOREM 3.2. The equation $q_n(a) = 2X^2$ has

a) one solution $n = 0$.

Proof.(i) By (3.13) if $q_n(a) = 2X^2$ then $3|n$. Put $n = 3m$. Then by (3.9) - (3.12) we have

$$2X^2 = q_{3m}(a) = q_m(a)(q_m(a)^2 - 3)$$

where clearly $(q_m(a), q_m(a)^2 - 3) = 1$ or 3. This implies that $q_m(a)^2 - 3 = 2X_1^2$, $3X_1^2$, X_1^2, or $6X_1^2$, and it is easily seen that the first two possibilities are impossible modulo 8. Thus we require either

$$q_m(a)^2 - 3 = X_1^2, \; q_m(a) = 2X_2^2$$

where the first equation implies that $m = 0$, or

$$q_n(a)^2 - 3 = 6X_1^2, \; q_m(a) = 3X_2^2.$$

The first equation clearly implies that $q_m(a)$ is odd and so from the second equation $q_m(a) \equiv 3 \pmod 8$. But now from (3.16), if m is even,

$$q_m(a) \equiv q_0(a) \text{ or } q_{\pm 2}(a) \pmod 8$$

i.e.

$$q_m(a) \equiv 2 \text{ or } 7 \pmod 8$$

Hence, if $q_{3m}(a) = 2X^2$ then $m = 0$ or m is odd.
But from (3.16) similarly, if m is odd

$$q_m(a) \equiv q_{\pm 1}(a) \text{ or } q_3(a) \pmod 8$$

i.e.

$$q_m(a) \equiv a \text{ or } -2a \pmod 8.$$

Thus if $q_{3m}(a) = 2X^2$, and $m \neq 0$, then $a \equiv 3 \pmod 8$ and m is odd.
(ii) Suppose now that m is odd and $a \equiv 3 \pmod 8$. Then n is odd and if $n \neq \pm 3$ we may write $n = \pm 3 + 2.3^r.k$ as usual. Then by repeated applications of (3.23) we find

$$q_n(a) \equiv -q_{\pm 3}(a) \pmod{q_k(a)}$$

whence, by virtue of (3.7)

$$(2q_n(a) / q_k(a)) = (-2q_3(a) / q_k(a)) = -(2q_3(a) / q_k(a))$$

by (3.17)

$$= -1 \text{ by (3.30)}$$

since $a \equiv 3 \pmod 8$.
Thus $q_n(a) \neq 2X^2$ except possibly for $n = \pm 3$, $a \equiv 3 \pmod 8$.
(iii) Suppose now that $2X^2 = a(a^2 - 3) = q_{\pm 3}(a)$. Then as in (i) we have

$$a = 3X_1^2, \quad a^2 - 3 = 6X_2^2$$

or

$$2X_2^2 = 3X_1^4 - 1.$$

But from (1) again this equation has only the solutions $X_1 = 1$ or 3 giving $a = 3$ or 27. Since by (3.8) $a \geq 5$, $a = 27$ is the only possibility, but $a = 27$ gives $d = 29$ and the equation $X^2 - 29Y^2 = -4$ has solutions. Thus $q_{\pm 3}(a) \neq 2X^2$ in this case. This completes the proof.

THEOREM 3.3. The equation $p_n(a) = Y^2$ has

a) three solutions $n = 0, 1, 2$ if a is a perfect square;

b) two solutions $n = 0, 1$ otherwise.

Proof. (i) If n is odd, $p_n(a) \neq Y^2$ except for $n = 1$. For $p_1(a) = 1 = 1^2$, $p_3(a) = a^2 - 1 \neq Y^2$ since $a \geq 5$ by (3.8), and if $n \neq 1$ or 3 we may write $n = t + 2.3^r.k$ where $2 \mid k$, $3 \nmid k$ and $t = 1$ or 3. Repeated applications of (3.22) now give

$$p_n(a) \equiv (-1)3^r p_t(a) \equiv -p_t(a) \pmod{q_k(a)}$$

Thus by (3.31) with $n = 1$,

$$(p_n(a) / q_k(a)) = (-p_1(a) / q_k(a)) = -1 \text{ by (3.17)}$$

Thus $p_n(a) \neq Y^2$ except for $n = 1$.

(ii) Suppose now that n is even and $p_n(a) = Y^2$. Then from (3.9)

$$Y^2 = p_n(a) = p_{\frac{1}{2}n}(a)\, q_{\frac{1}{2}n}(a)$$

and so, by virtue of (3.14) we have either

$$p_{\frac{1}{2}n}(a) = Y_1^2, \quad q_{\frac{1}{2}n}(a) = Y_2^2$$

or

$$p_{\frac{1}{2}n}(a) = 2Y_1^2, \quad q_{\frac{1}{2}n}(a) = 2Y_2^2$$

From theorem 3.1 the first case is possible only for $\frac{1}{2}n = \pm 1$, a is a perfect square. Since $p_{-1}(a) = -1$ the only solution is therefore $n = 2$, a is a perfect square.

The second case is possible only for $n = 0$, from theorem 3.2.

This completes the proof of the theorem.

THEOREM 3.4. The equation $p_n(a) = 2Y^2$ has

a) two solutions $n = 0, 3$ if $a = \frac{1}{2}Q_{2n}(2)$

b) one solution $n = 0$ otherwise.

Proof.(i) From part (i) of the proof of theorem 3.3 we see that if n is odd and $n \neq 1$ or 3 then there exists k such that $2|k$, $3\nmid k$ and

$$(p_n(a) / q_k(a)) = -1.$$

But then, since $q_k(a) \equiv 7 \pmod 8$ from (3.17)

$$(2p_n(a) / q_k(a)) = -1$$

Hence $p_n(a) \neq 2Y^2$ except possibly for $n = 1$ or 3. But $p_1(a) = 1 \neq 2Y^2$ and so the only possibility is $n = 3$. But then $a^2 - 1 = 2Y^2$, i.e. $a = \frac{1}{2}Q_{2n}(2)$.

(ii) Suppose now that n is even. Then if $p_n(a) = 2Y^2$, from (3.9)

$$2Y^2 = p_{\frac{1}{2}n}(a)\ q_{\frac{1}{2}n}(a)$$

and so by (3.14) we have either

$$p_{\frac{1}{2}n}(a) = 2Y_1^2 \ ; \ q_{\frac{1}{2}n}(a) = Y_2^2$$

or

$$p_{\frac{1}{2}n}(a) = Y_1^2 \ ; \ q_{\frac{1}{2}n}(a) = 2Y_2^2$$

The first case is impossible since the first equation requires $3|\frac{1}{2}n$ from (3.14) and the second requires $3\nmid n$ from theorem 3.1 In the second case, from theorem 3.2, the second equation is

satisfied only by $\frac{1}{2}n = 0$. Thus $n = 0$ is the only solution in this case.

This completes the proof.

Now we are seeking solutions of the equations $p_n(a) = Y^2$, NY^2 and $q_n(a) = X^2$, NX^2 where N is a square-free integer, and have dealt with the cases $p_n(a) = Y^2$, $2Y^2$ and $q_n(a) = X^2$, $2X^2$ in theorems 3.1 - 3.4. As in chapter 1 it turns out next to be most profitable to drop the restriction that N be square-free and consider $N = p_m(a)$, $2p_m(a)$, $q_m(a)$ and $2q_m(a)$. Again, we must first establish for what values of n $p_m(a) \mid p_n(a)$ and the corresponding results for the other functions. The results are contained in the following six lemmas.

LEMMA 3.1. $p_m(a) \mid p_{rm}(a)$ for all integers r.

Proof. From (3.20) we have

$$p_{rm}(a) \equiv p_{(r-2)m}(a) \equiv \cdots \equiv \begin{cases} p_o(a) & \text{if r is even} \\ p_m(a) & \text{if r is odd} \end{cases} \pmod{p_m(a)}$$

Thus since $p_o(a) = 0$, $p_m(a) \mid p_{rm}(a)$ for all integers r.

LEMMA 3.2. $q_m(a) \mid q_{rm}(a)$ for any odd integer r.

Proof. From (3.19) if r is odd we have

$$q_{rm}(a) \equiv -q_{(r-2)m}(a) \equiv \cdots \equiv \pm q_m(a) \pmod{q_m(a)}$$

and thus, if r is odd, $q_m(a) \mid q_{rm}(a)$.

LEMMA 3.3. $(q_{rm}(a), q_m(a)) = 1$ or 2 for every integer r.

Proof. If r is even from (3.19) we have

$$q_{rm}(a) \equiv \pm q_o(a) = \pm 2 \pmod{q_m(a)}.$$

Hence the result.

LEMMA 3.4. $p_{(m,n)}(a) = (p_m(a), p_n(a))$.

Proof. Let $(m,n) = r$. Then it is well-known that there exist integers g and h such that $gm + hn = r$. Thus from (3.9) we find that

$$2p_r(a) = p_{gm}(a)q_{hn}(a) + p_{hn}(a)q_{gm}(a) \qquad (')$$

From lemma 3.1 $p_m(a) \mid p_{gm}(a)$ and $p_n(a) \mid p_{hn}(a)$. Thus $(p_m(a), p_n(a)) \mid 2p_r(a)$.

But also from lemma 3.1 $p_r(a) \mid p_n(a)$ and $p_r(a) \mid p_m(a)$. Hence $(p_m(a), p_n(a)) = p_r(a)$ or $2p_r(a)$. Obviously, if $p_m(a)$ or $p_n(a)$ is odd, $(p_m(a), p_n(a)) = p_r(a)$. If they are both even, by lemma 3.1, $p_{gm}(a)$ and $p_{hn}(a)$ are also both even. Then from (3.13), $q_{gm}(a)$ and $q_{hn}(a)$ are both even. Thus from (') we may obtain

$$p_r(a) = p_{gm}(a)\,(\tfrac{1}{2}q_{hn}(a)) + p_{hn}(a)\,(\tfrac{1}{2}q_{gm}(a))$$

where $\frac{1}{2}q_{hn}(a)$ and $\frac{1}{2}q_{gm}(a)$ are both integers. Then again, as above, $(p_m(a), p_n(a)) = p_r(a)$.

This completes the proof.

LEMMA 3.5. Let $(m,n) = r$ and let $\frac{n}{r}$ be odd. Then

a) if $\frac{m}{r}$ is odd $(q_m(a), q_n(a)) = q_r(a)$

b) if $\frac{m}{r}$ is even $(q_m(a), q_n(a)) = 1$ or 2.

Proof. Since $(m,n) = r$ there exist integers g and h such that $gm + hn = r$. Then from (3.10) we find

$$2q_r(a) = (a^2 - 4)p_{gm}(a)p_{hn}(a) + q_{gm}(a)q_{hn}(a) \qquad ('')$$

(a) If $\frac{m}{r}$ and $\frac{n}{r}$ are both odd, g and h will be of opposite parity. We may suppose, without loss of generality that g is odd. Then from lemma 3.2 $q_m(a) \mid q_{gm}(a)$. Since h is even, from

lemma 3.1 and (3.9),

$p_{2n}(a) = q_n(a)\, p_n(a) \mid p_{hn}(a)$ and hence $(q_m(a), q_n(a)) \mid 2q_r(a)$. Since $\frac{m}{r}$ and $\frac{n}{r}$ are both odd, from lemma 3.2 also $q_r(a) \mid q_m(a)$ and $q_r(a) \mid q_n(a)$. Thus $(q_m(a), q_n(a)) = q_r(a)$ or $2q_r(a)$. By a method similar to that used at the end of the proof of lemma 3.4 we may show that $(q_m(a), q_n(a)) \neq 2q_r(a)$.

This completes the proof of (a).

(b) If $\frac{m}{r}$ is even, then h must be odd.

(i) If g is even as above we may show that $(q_m(a), q_n(a)) \mid 2q_r(a)$. Also, since $\frac{n}{r}$ is odd, by lemma 3.2 $q_r(a) \mid q_n(a)$. Thus $(q_m(a), q_n(a))$ divides $(q_m(a), 2q_r(a))$. But since $\frac{m}{r}$ is even, from lemma 3.3, $(q_m(a), q_r(a)) \mid 2$. Thus $(q_m(a), 2q_r(a)) \mid 4$. But since m is even, from (3.11), $q_m(a) = q_{\frac{1}{2}m}(a)^2 - 2$ and so $q_m(a)$ is either odd or congruent to 2 modulo 4. Thus $(q_m(a), q_n(a)) \mid 2$.

(ii) If g is odd from (3.9) we have

$$2p_r(a) = p_{gm}(a)\, q_{hn}(a) + p_{hn}(a)\, q_{gm}(a) \qquad (')$$

where from lemma 3.2 $q_m(a) \mid q_{gm}(a)$ and $q_n(a) \mid q_{hn}(a)$. Thus $(q_m(a), q_n(a)) \mid 2p_r(a)$. Since m is even, however, from (3.11) and (3.12) $q_m(a) \equiv 2 \pmod{p_{\frac{1}{2}m}(a)}$. From lemma 3.1 $p_r(a) \mid p_{\frac{1}{2}m}(a)$ and hence $(q_m(a), q_n(a)) \mid 4$ but as above $(q_m(a), q_n(a)) = 4$ is impossible.

This completes the proof.

LEMMA 3.6. Let $(m,n) = r$. Then

(a) if $\frac{m}{r}$ is odd, $(p_m(a), q_n(a)) \mid 4$;

(b) if $\frac{m}{r}$ is even, $(p_m(a), q_n(a)) = q_r(a)$.

Proof. Again, since $(m,n) = r$ there exists integers g and h such that $gm + hn = r$ and from (3.9) and (3.10) we obtain as before

$$2p_r(a) = p_{gm}(a)\, q_{hn}(a) + p_{hn}(a)\, q_{gm}(a) \qquad (')$$

$$2q_r(a) = (a^2 - 4)\, p_{gm}(a)\, p_{hn}(a) + q_{gm}(a)\, q_{hn}(a) \qquad ('')$$

(a)(i) If $\frac{m}{r}$ is odd and h is odd, from lemmas 3.1 and 3.2, $p_m(a) | p_{gm}(a)$ and $q_n(a) | q_{hn}(a)$. Thus from ('') $(p_m(a), q_n(a)) | 2q_n(a)$. But since $\frac{m}{r}$ isodd, $q_r(a) | q_m(a)$ and so from (3.12) it is easily seen that $(p_m(a), q_r(a)) = 1$ or 2.
Thus $(p_m(a), q_n(a)) | 4$ as required.

(ii) If $\frac{m}{r}$ is odd and h is even, from lemma 3.1 and (3.9) we see that $p_m(a)\ p_{gm}(a)$ and $p_{2n}(a) = p_n(a)\ q_n(a) | p_{hn}(a)$. Thus from ('), $(p_m(a), q_n(a)) | 2p_r(a)$. But from lemma 3.1 $p_r(a) | p_n(a)$ and thus, by (3.12) $(p_r(a), q_n(a)) = 1$ or 2. Thus again $(p_m(a), q_n(a)) | 4$ as required.
This concludes the proof of (a).

(b) If $\frac{m}{r}$ is even, then h must be odd. Then from ('') as in the proof of (a) (i) $(p_m(a), q_n(a)) | 2q_r(a)$. But now, from the definition of r, since $\frac{m}{r}$ is even, $\frac{n}{r}$ is odd. Thus from lemma 3.2 $q_r(a) | q_n(a)$. Also, since $\frac{m}{r}$ is even, from lemma 3.1 and (3.9) $p_{2r}(a) = p_r(a)\ q_r(a) | p_m(a)$. Hence $(p_m(a), q_n(a)) = q_r(a)$ or $2q_r(a)$. But an arguement similar to that at the end of the proof of lemma 3.4 shows that $(p_m(a), q_n(a)) = 2q_r(a)$ is impossible.

This completes the proof.

COROLLARY 3.1. (of lemmata 3.4 - 3.6)

(a) If $p_m(a) | p_n(a)$ then $m | n$.

(b) If $q_m(a) | q_n(a)$ and $|q_m(a)| > 2$, then $\frac{n}{m}$ is an odd integer.

(c) If $q_m(a) | p_n(a)$ and $|q_m(a)| > 2$, then $\frac{n}{m}$ is an even integer.

(d) If $p_m(a) | q_n(a)$ and $|p_m(a)| > 2$, then $m = 2$.

Proof. These results follow immediately from lemmata 3.4 - 3.6.

We are now in a position to solve the equations $p_n(a) = p_m(a)Y^2$, $2p_m(a)Y^2$, $q_m(a)Y^2$, $2q_m(a)Y^2$ and $q_n(a) = q_m(a)X^2$, $2q_m(a)X^2$, $p_m(a)X^2$, $2p_m(a)X^2$. The results are contained in

theorems 3.5 - 3.12.

THEOREM 3.5. For any given $m \neq 0, q_n(a)$ is of the form $q_m(a)X^2$ only for $n = \pm m$.

Proof. We note first that from corollary 3.1 if $q_n(a) = q_m(a)X^2$ then $n = mt$ for some odd integer t.

(i) If $t = \pm 1$, then $q_n(a) = q_m(a) = q_m(a)1^2$, from (3.7), whereas if $t \neq \pm 1$, we may write $n = \pm m + 2.3^r.k$ where $2 \mid k$, $3 \nmid k$. Repeated applications of (3.23) now give

$$q_n(a) \equiv (-1)^r q_{\pm m}(a) \pmod{q_k(a)}$$

Now if 2^s is the highest power of 2 which divides $m, 2^s + 1 \mid k$ and so, since $3 \nmid k$, from lemma 3.5 and (3.13) $(q_m(a), q_k(a)) = 1$. Thus by virtue of (3.7)

$$\begin{aligned}(q_m(a)\, q_n(a) / q_k(a)) &= (-q_m(a)^2 / q_k(a)) \\ &= -1 \text{ by (3.17)}\end{aligned}$$

Thus $q_n(a) \neq q_m(a)X^2$.

This completes the proof.

THEOREM 3.6. For any given $m \neq 0, q_n(a)$ is never of the form $2q_m(a)X^2$.

Proof. Again, from corollary 3.1 we see that if $q_n(a) = 2q_m(a)X^2$, then $n = mt$ for some odd integer t. But then, as in the proof of theorem 3.5, if $t \neq \pm 1$, this implies that there exists k such that $2 \mid k$, $3 \nmid k$ and

$$(q_m(a)\, q_n(a) / q_k(a)) = -1.$$

Since, from (3.17), $q_k(a) \equiv 7 \pmod 8$, therefore

$$(2q_m(a)\, q_n(a) / q_k(a)) = -1.$$

and thus, if $t \neq \pm 1$, $q_n(a) \neq 2q_m(a)\,X^2$. If $t = \pm 1$, $q_n(a) = q_m(a) \neq 2q_m(a)\,X^2$.

This completes the proof.

THEOREM 3.7. For any given $m \neq 0,1$ $p_n(a)$ is of the form $p_m(a)Y^2$ only for $n = m$ and $n = 0$.

Proof. We note first, that from corollary 3.1, if $p_n(a) = p_m(a)Y^2$ then $n = mt$ for some integer t.

(i) If t is even $p_n(a) \neq p_m(a)Y^2$ except for $n = 0$. For, let $t = 2t'$ and then from (3.9)

$$p_n(a) = p_{mt'}(a)\, q_{mt'}(a)$$

where, from (3.14), $(p_{mt'}(a), q_{mt'}(a)) = 1$ or 2. But by lemma 3.1, $p_m(a) \mid p_{mt'}(a)$ and therefore, if $p_n(a) = p_m(a)Y^2$ we require either

$$p_{mt'}(a) = p_m(a)Y_1^2 \; ; \; q_{mt'}(a) = Y_2^2$$

which from theorem 3.1 is impossible since $|mt'| > 1$, or

$$p_{mt'}(a) = 2p_m(a)Y_1^2 \; ; \; q_{mt'}(a) = 2Y_2^2$$

From theorem 3.2 this requires $mt' = 0$, and hence if t is even, $p_n(a) = p_m(a)\,Y^2$ if and only if $n = 0$.

(ii) If t is odd and m is even, $p_n(a) \neq p_m(a)Y^2$ except for $t = 1$. For clearly $p_m(a) = p_m(a).1^2$ whereas if $t \neq 1$, put $m = 2m'$ and from (3.9) we have

$$p_n(a) = p_{m't}(a)\, q_{m't}(a)$$

where, by (3.14), $(p_{m't}(a), q_{m't}(a)) = 1$ or 2. Also, since t is odd, from lemmas 3.1 and 3.2 $p_{m'}(a) \mid p_{m't}(a)$ and $q_{m'}(a) \mid q_{m't}(a)$. From (3.9) $p_m(a) = p_{m'}(a)\, q_{m'}(a)$ and so, if

$p_n(a) = p_m(a)Y^2$ we require either

$$p_{m't}(a) = 2p_{m'}(a)Y_1^2 \; ; \; q_{m't}(a) = 2q_{m'}(a)Y_2^2$$

which is impossible from theorem 3.6, or

$$p_{m't}(a) = p_{m'}(a)Y_1^2 \; ; \; q_{m't}(a) = q_{m'}(a)Y_2^2$$

From theorem 3.5 the second equation implies $t = \pm 1$, but $p_{-m}(a) = -p_m(a)$.

Thus $t = 1$ is the only solution.

(iii) If $2\nmid m$, $3\nmid m$ and t is odd then $p_n(a) \neq p_m(a)Y^2$, except for $t = 1$. For clearly $p_{m_2}(a) = p_m(a).1^2$ and $p_{3m}(a) = p_m(a)\,(q_m(a)^2 - 1) \neq p_m(a)Y^2$ from (3.35) and if $t \neq 1$ or 3 we may write $n = sm + 2.3^r.km$ where $2|km$, $3\nmid km$ and $s = 1$ or 3. Repeated applications of (3.22) now give

$$p_n(a) \equiv -p_{sm}(a) \pmod{q_{km}(a)}$$

Now if 2^u is the highest power of 2 which divides m, $2^{u+1}|k$ and so, by lemma 3.6 and (3.13) $(p_{sm}(a), q_{km}(a)) = 1$. Thus

$$\begin{aligned}(p_n(a)\, p_m(a) / q_{km}(a)) &= (-p_m(a)\, p_{sm}(a) / q_{km}(a)) \\ &= -(p_m(a)^2 / q_{km}(a)) \text{ by (3.17),(3.31)} \\ &= -1\end{aligned}$$

Thus $p_n(a) \neq p_m(a)Y^2$ except for $t = 1$.

(iv) If $2\nmid m$, $3|m$ and $2\nmid t$, $3|t$, then $p_n(a) \neq p_m(a)Y^2$. For, from (3.9)

$$p_n(a) = p_{jmt}(a)\,(q_{jmt}(a)^2 - 1)$$

where, since $3|t$ by lemma 3.1 $p_m(a) | p_{\frac{1}{3}mt}(a)$ and also, from (3.12), $(p_{\frac{1}{3}mt}(a), q_{\frac{1}{3}mt}(a)^2 - 1) = 1$ or 3. Thus if $p_n(a) = p_m(a)Y^2$ we require either

$$p_{\frac{1}{3}mt}(a) = p_m(a)\, Y_1^2 \; ; \; q_{\frac{1}{3}mt}(a)^2 - 1 = Y_2^2$$

which is impossible since mt is odd, or

$$p_{\frac{1}{3}mt}(a) = 3p_m(a)\, Y_1^2 \; ; \; q_{\frac{1}{3}mt}(a)^2 - 1 = 3Y_2^2$$

But either $3|a = p_2(a)$ or $3|a^2 - 1 = p_3(a)$ and since we require $3| p_{\frac{1}{3}mt}(a)$ where mt is odd, therefore from lemma 3.1 $3|a^2 - 1$ and $3\nmid a$. Hence, by (3.34) the second equation is impossible and so $p_n(a) \neq p_m(a)Y^2$.

(v) If $2\nmid m$, $3|m$ and $2\nmid t$, $3\nmid t$ then $p_n(a) \neq p_m(a)Y^2$ except for $t = 1$. For we put $m = 3m'$ and from (3.9) and (3.11) we find

$$p_n(a) = p_{m't}(a)\, (q_{m't}(a)^2 - 1)$$

$$p_m(a) = p_{m'}(a)\, (q_{m'}(a)^2 - 1)$$

where $(p_{m't}(a), q_{m't}(a)^2 - 1) = 1$ or 3 and since $3\nmid t$ $(p_{m't}(a), p_m(a)) = p_{m'}(a)$ by lemma 3.4. Thus if $p_n(a) = p_m(a)Y^2$ we require either

$$p_{m't}(a) = 3p_{m'}(a)Y_1^2 \; ; \; q_{m't}(a)^2 - 1 = 3(q_{m'}(a)^2 - 1)Y_2^2$$

where as in the proof of (iv) we can show that this requires $3|m't$ since $2\nmid m't$ and then, from (3.13) the second equation is impossible modulo 8, or

$$p_{m't}(a) = p_{m'}(a)\, Y_1^2 \; ; \; q_{m't}(a)^2 - 1 = (q_{m'}(a)^2 - 1)Y_2^2$$

From (iii) the first equation implies $t = 1$ unless $3|m'$. If $3|m'$ we require $p_{m't}(a) = p_{m'}(a)Y_1^2$ where $2\nmid m'$, $3\nmid m'$ and $2\nmid t$, $3\nmid t$ and so have the same situation as we started with. We may

repeat the above arguement until all factors of 3 in m are exhausted. Finally we arrive at an equation

$$p_{m^{(r)}t}(a) = p_{m^{(r)}}(a)Y_s^2$$

where $3\nmid m^{(r)}$ and t is odd. From (iii) this now implies t = 1. This completes the proof of the theorem.

THEOREM 3.8. For any given $m \neq 0,1$ $p_n(a)$ is of the form $2p_m(a)Y^2$ only for n = 0.

Proof. We note again that if $p_n(a) = 2p_m(a)Y^2$ then n = mt for some integer t, from corollary 3.1.

(i) If t is even, $p_n(a) = 2p_m(a)Y^2$ only for n = 0. For, from (3.9) and (3.14),

$$p_n(a) = p_{\frac{1}{2}mt}(a)\, q_{\frac{1}{2}mt}(a)$$

where $(p_{\frac{1}{2}mt}(a), q_{\frac{1}{2}mt}(a)) = 1$ or 2. Also, since t is even, from lemma 3.1 $p_m(a) \mid p_{\frac{1}{2}mt}(a)$. Thus if $p_n(a) = 2p_m(a)Y^2$ we need

$$q_{\frac{1}{2}mt}(a) = Y_1^2 \text{ or } 2Y_1^2$$

From theorems 3.1 and 3.2, since $m \neq 0,1$ the only possibility is $q_0(a) = 2$ and this gives the stated result.

(ii) If $2\nmid t$ but $2 \mid m$ then $p_n(a) \neq 2p_m(a)Y^2$. For, from (3.9) and (3.14)

$$p_n(a) = p_{\frac{1}{2}mt}(a)\, q_{\frac{1}{2}mt}(a)$$

where $(p_{\frac{1}{2}mt}(a), q_{\frac{1}{2}mt}(a)) = 1$ or 2. Since t is odd, by lemmas 3.1 and 3.2 $p_{\frac{1}{2}m}(a) \mid p_{\frac{1}{2}mt}(a)$ and $q_{\frac{1}{2}m}(a) \mid q_{\frac{1}{2}mt}(a)$. From (3.9) $p_m(a) = p_{\frac{1}{2}m}(a)\, q_{\frac{1}{2}m}(a)$ and so, if $p_n(a) = 2p_m(a)Y^2$ we require either

$$q_{\frac{1}{2}mt}(a) = 2q_{\frac{1}{2}m}(a)Y_1^2$$

which is impossible from theorem 3.6, or

$$q_{\frac{1}{2}mt}(a) = q_{\frac{1}{2}m}(a)Y_1^2 \; ; \; p_{\frac{1}{2}mt}(a) = 2p_{\frac{1}{2}m}(a)\, Y_2^2$$

However, from theorem 3.5 the first equation requires $t = 1$ and $p_{\frac{1}{2}m}(a) \neq 2p_{\frac{1}{2}m}(a)Y^2$.

Thus $p_n(a) \neq 2p_m(a)Y^2$ in this case.

(iii) If $2\nmid t$, $3 \mid t$ and $2\nmid m$ then $p_n(a) \neq 2p_m(a)Y^2$. For if we put $t = 3t'$ from (3.9) and (3.11) we find that

$$p_n(a) = p_{t',m}(a)\,(q_{t',m}(a)^2 - 1)$$

where, from (3.12) $(p_{t',m}(a),\, q_{t',m}(a)^2 - 1) = 1$ or 3. Since $3 \mid t$, by lemma 3.1 $p_m(a) \mid p_{t',m}(a)$ and so if $p_n(a) = 2p_m(a)Y^2$ there are four possibilities:

(a) $q_{t',m}(a)^2 - 1 = Y_1^2$, which is impossible since mt is odd.

(b) $q_{t',m}(a)^2 - 1 = 2Y_1^2$, which, since $m \neq 1, 2\nmid mt$, from (3.32) implies $3 \mid mt$. But then from (3.13) this is impossible modulo 8.

(c) $q_{t',m}(a)^2 - 1 = 3Y_1^2$; $p_{t',m}(a) = 6p_m(a)Y_2^2$, which, since $3 \mid a = p_2(a)$ or $3 \mid a^2 - 1 = p_3(a)$, from lemma 3.1 implies $3 \mid a^2 - 1$, $3\nmid a$. But then the first equation is impossible from (3.34).

(d) $q_{t',m}(a)^2 - 1 = 6Y_1^2$; $p_{t',m}(a) = 3p_m(a)Y_2^2$, which is impossible also by the same arguement as that used in (c).

Thus $p_n(a) \neq 2p_m(a)Y^2$ in this case.

(iv) If $2\nmid t$, $3\nmid t$ and $2\nmid m$ then $p_n(a) \neq 2p_m(a)Y^2$. For, if $p_n(a) = 2p_m(a)Y^2$ by (3.13) $3 \mid mt$ and since $3\nmid t$ therefore $3 \mid m$. Let $m = 3m'$. Then from (3.9) and (3.11) we have

$$p_n(a) = p_{m',t}(a)\,(q_{m',t}(a)^2 - 1)$$

$$p_m(a) = p_{m'}(a)\,(q_{m'}(a)^2 - 1)$$

where $(p_{m't}(a), q_{m't}(a)^2 - 1) = 1$ or 3 and since $3 \nmid t$, by lemma 3.4 $(p_{m't}(a), p_m(a)) = p_{m'}(a)$. Thus if $p_n(a) = 2p_m(a)Y^2$ we have four possibilities:

(a) $p_{m't}(a) = p_{m'}(a)Y_1^2$; $q_{m't}(a)^2 - 1 = 2(q_{m'}(a)^2 - 1)Y_2^2$
where, from theorem 3.7 the first equation requires $t = 1$ which is impossible for the second.

(b) $p_{m't}(a) = 3p_{m'}(a)Y_1^2$; $q_{m't}(a)^2 - 1 = 6(q_{m't}(a)^2 - 1)Y_2^2$,
which, since $3 \mid a = p_2(a)$ or $3 \mid a^2 - 1 = p_3(a)$ and mt is odd implies $3 \mid m't$ from lemma 3.1. But then from (3.13) the second equation is impossible modulo 4.

(c) $p_{m't}(a) = 6p_{m't}(a)Y_1^2$; $q_{m't}(a)^2 - 1 = 3(q_{m'}(a)^2 - 1)Y_2^2$
where, from (3.13) the first equation requires $3 \mid m't$ and the second is impossible modulo 4.

(d) $p_{m't}(a) = 2p_{m'}(a)Y_1^2$; $q_{m't}(a)^2 - 1 = (q_{m'}(a)^2 - 1)Y_2^2$
where, from (3.13) the first equation requires $3 \mid m'$. Thus we have again the situation with which we started and may repeat the above process until we arrive at an equation $p_{m/3^s}(a) = 2p_{m/3^s}(a)Y_1^2$ where $3 \nmid \frac{m}{3^s}$ which is clearly impossible from (3.13). This completes the proof of the theorem.

THEOREM 3.9. For any given $m \neq 0$, $p_n(a)$ is of the form $q_m(a)Y^2$ only for ($n = 2$, $m = \pm 1$), (a = a perfect square, $n = 4$, $m = \pm 2$) and $n = 0$.

Proof. First we note that from corollary 3.1 if $p_n(a) = q_m(a)Y^2$ then $n = 2mt$ for some integer t. Thus by (3.9) and (3.14)

$$p_n(a) = p_{mt}(a)\, q_{mt}(a)$$

where $(p_{mt}(a), q_{mt}(a)) = 1$ or 2.

(i) If t is odd, by lemma 3.2 $q_m(a) \mid q_{mt}(a)$ and so if $p_n(a) = q_m(a)Y^2$ we require either

$$p_{mt}(a) = 2Y_1^2 \; ; \; q_{mt}(a) = 2q_m(a)\, Y_2^2$$

where from theorem 3.6 the second equation is impossible, or

$$p_{mt}(a) = Y_1^2 \; ; \; q_{mt}(a) = q_m(a)\, Y_2^2$$

where from theorem 3.3 since $m \neq 0$ and t is odd, the first equation requires $mt = 1$ or $mt = 2$, a = a perfect square. These possibilities give the stated results.

(ii) If t is even, by lemma 3.1 and (3.9) $p_{2m}(a) = p_m(a)\, q_m(a) \mid p_{tm}(a)$ and so if $p_n(a) = q_m(a)Y^2$ we require $q_{mt}(a) = Y_1^2$ or $2Y_1^2$ where mt is even. From theorems 3.1 and 3.2 this is only possible for $t = 0$.

This completes the proof.

THEOREM 3.10. For any given $m \neq 0$, $p_n(a)$ is of the form $2q_m(a)\, Y^2$ only for $n = 0$ and ($a = \frac{1}{2}Q_{2n}(2)$, $n = 6$, $m = \pm 3$).

Proof. As in the proof of theorem 3.9 we require $n = 2mt$ and

$$p_n(a) = p_{mt}(a)\, q_{mt}(a)$$

where $(p_{mt}(a), q_{mt}(a)) = 1$ or 2.

(ii) If t is odd, from lemma 3.2 $q_m(a) \mid q_{mt}(a)$ and if $p_n(a) = 2q_m(a)Y^2$ we require either

$$p_{mt}(a) = Y_1^2 \; ; \; q_{mt}(a) = 2q_m(a)Y_2^2$$

where from theorem 3.6 the second equation is impossible, or

$$p_{mt}(a) = 2Y_1^2 \; ; \; q_{mt}(a) = q_m(a)Y_2^2$$

where from theorem 3.4 since $m \neq 0$ and t is odd, the first equation requires $mt = 3$, $a = \frac{1}{2}Q_{2n}(2)$, which gives the stated result.

(ii) If t is even as in the proof of theorem 3.9 (ii) we see

that we require $q_{mt}(a) = Y_1^2$ or $2Y_1^2$ where mt is even and from theorems 3.1 and 3.2 again this is possible only for t = 0.

This completes the proof.

THEOREM 3.11. For any given $m \neq 0$, 1 $q_n(a)$ is of the form $p_m(a)X^2$ only for ($n = \pm 1$, $m = 2$).

Proof. From corollary 3.1 we see that if $q_n(a) = p_m(a)X^2$ then m = 2. But $p_2(a) = q_{\pm 1}(a)$ and so the result follows from theorem 3.5.

This completes the proof.

THEOREM 3.12. For any given $m \neq 0$, 1 $q_n(a)$ is never of the form $2p_m(a)X^2$.

Proof. From corollary 3.1 again we see that if $q_n(a) = 2p_m(a)X^2$ then m = 2. But $p_2(a) = q_{\pm 1}(a)$ and the result follows from theorem 3.6.

This completes the proof.

The following results will be required later and are a direct consequence of theorems 3.1 - 3.12.

COROLLARY 3.2. (of theorems 3.1 - 3.12)

(a) If $m \geq n \geq 2$, $p_m(a)\ p_n(a)$ is a square only for m = n.

$2p_m(a)\ p_n(a)$ is never a square.

(b) If $m \geq n \geq 1$, $q_m(a)\ q_n(a)$ is a square only for $m = \pm n$.

$2q_n(a)\ q_m(a)$ is never a square.

(c) If $m \geq 1$, $n \geq 2$, then $p_n(a)\ q_m(a)$ is a square only for ($m = \pm 1$, n = 2) and (a = a perfect square, $m = \pm 2$, n = 4).

$2p_n(a)\ q_m(a)$ is a square only for ($a = \frac{1}{2}Q_{2n}(2)$, $m = \pm 3$, n = 6).

Proof. (a) From lemma 3.4, $(p_m(a), p_n(a)) = p_{(m,n)}(a)$ and therefore, if $p_m(a)\ p_n(a) = Y^2$ we must have $p_n(a) = p_{(m,n)}(a)Y_1^2$, $p_m(a) = p_{(m,n)}(a)Y_2^2$. If $(m,n) \geq 2$ from theorem 3.7 therefore, $m = (m,n) = n$. If $(m,n) = 1$, since $m \geq n \geq 2$ from theorem 3.3

the only possibility is m = 3 and n = 3, but then (m,n) ≠ 1.

Similarly, $2p_m(a)\, p_n(a) = Y^2$ implies either

$$p_m(a) = 2p_{(m,n)}(a)\, Y_1^2 \; ; \; p_n(a) = p_{(m,n)}(a) Y_2^2$$

or

$$p_m(a) = p_{(m,n)}(a) Y_1^2 \; ; \; p_n(a) = 2p_{(m,n)}(a) Y_2^2$$

If $(m,n) \geq 2$, from theorems 3.7 and 3.8 there are no solutions whereas if $(m,n) = 1$ from theorems 3.3 and 3.4 the only possibility is ($a = t^2$, $a^2 - 1 = 2z^2$, $m = 3$, $n = 2$) but since $a \geq 5$ from theorem 2.1 no integer satisfies the conditions for a. b) and c) follow in a similar way from theorems 3.1 - 3.12.

We have now solved the equations $p_n(a) = NY^2$ and $q_n(a) = NX^2$ in the cases where $N = p_m(a)$, $2p_m(a)$, $q_m(a)$ and $2q_m(a)$. We wish to solve them for general square-free values of N but it is convenient to consider one more special case before proceeding to the solution in the general case. Here again we do not confine ourselves to square-free values.

It is obvious that, from (3.12), since a is odd, $(q_n(a), a^2 - 4) = 1$ and that therefore if $q_n(a) = RX^2$ and $R \mid a^2 - 4$, then $R = 1$. The following result however is not so trivial.

THEOREM 3.13. Let R be an integer greater than 1 such that $R \mid a^2 - 4$. Then the equation $p_n(a) = RY^2$ has only the solutions $n = 0$ and possibly $n = R = 3$.

Proof. From (3.27) and (3.28) we see first that $R \mid p_n(a)$ if and only if $R \mid n$. Let $n = mR$.

(i) Suppose that m is even. Then $p_n(a) = RY^2$ only for $n = 0$. For, from (3.9), if $p_n(a) = RY^2$

$$Ry^2 = p_{\frac{1}{2}mR}(a)\, q_{\frac{1}{2}mR}(a)$$

where from (3.14) $(p_{\frac{1}{2}mR}(a), q_{\frac{1}{2}mR}(a)) = 1$ or 2. Also, from (3.27) and (3.28) since m is even, $R \mid p_{\frac{1}{2}mR}(a)$. Thus we must have either

$$p_{\frac{1}{2}mR}(a) = RY_1^2 \; ; \; q_{\frac{1}{2}mR}(a) = Y_2^2$$

where from theorem 3.1, since $R > 1$, the second equation has no solutions,

or

$$p_{\frac{1}{2}mR}(a) = 2RY_1^2 \; ; \; q_{\frac{1}{2}mR}(a) = 2Y_2^2$$

From theorem 3.2 the second equation requires $\frac{1}{2}mR = 0$ which gives the stated result.

(ii) Suppose that m is odd and $R \equiv 1$ or 3 (mod 8). Then $p_n(a) \neq RY^2$ except possibly for $m = 1$, $R = 3$. For if $mR \neq 3$, since $R > 1$, we may write $mR = t + 2.3^s.k$ where $2 \mid k$, $3 \nmid k$, and $t = 1$ or 3. Repeated applications of (3.22) now give

$$p_n(a) \equiv -p_t(a) \pmod{q_k(a)}$$

From lemma 3.6 and (3.13), $(p_t(a), q_k(a)) = 1$ and so

$$\begin{aligned} (Rp_n(a) \,/\, q_k(a)) = (-Rp_t(a) \,/\, q_k(a)) &= (-R \,/\, q_k(a)) \text{ by (3.31)} \\ &= -(R \,/\, q_k(a)) \text{ by (3.17)} \\ &= -(-q_k(a) \,/\, R) \text{ by (3.17)} \end{aligned}$$

But $2 \mid k$ and so by (3.25) $q_k(a) \equiv 2 \pmod{R}$. Thus, since $R \equiv 1$ or 3 (mod 8)

$$(Rp_n(a) \,/\, q_k(a)) = -(-2 \,/\, R) = -1.$$

and so $p_n(a) \neq RY^2$.

(iii) Suppose that m is odd and $R \equiv 5$ or 7 (mod 8). Then $p_n(a) \neq RY^2$. For we may write $mR = t + 2.3^s.k$ where $2 \mid k$, $3 \nmid k$ and

$t = -1$ or -3.

Then from (3.22) again

$$p_n(a) \equiv -p_t(a) \pmod{q_k(a)}$$

$$\equiv p_{-t}(a) \pmod{q_k(a)} \text{ by (3.6)}$$

As in (ii) $(p_t(a), q_k(a)) = 1$ and

$$(Rp_n(a) / q_k(a)) = (Rp_{-t}(a) / q_k(a)) = (R / q_k(a)) \text{ by (3.31)}$$

where once again $q_k(a) \equiv 2 \pmod{R}$. Thus since $R \equiv 5$ or $7 \pmod 8$,

$$(Rp_n(a) / q_k(a)) = (-2 / R) = -1.$$

and so $p_n(a) \neq RY^2$.

This completes the proof.

THEOREM 3.14. Let R be an integer greater than 1 such that $R \mid a^2 - 4$. Then the equation $p_n(a) = 2RY^2$ has only the solutions $n = 0$ and possibly $n = R = 3$.

Proof. From (3.27) and (3.28) again it is easily seen that $R \mid p_n(a)$ if and only if $R \mid n$. Let $n = mR$.

(i) Suppose that m is even. The $p_n(a) = 2RY^2$ only for $n = 0$. For from (3.9), if $p_n(a) = 2RY^2$ we have

$$2RY^2 = p_{\frac{1}{2}mR}(a)\ q_{\frac{1}{2}mR}(a)$$

where from (3.14) $(p_{\frac{1}{2}mR}(a), q_{\frac{1}{2}mR}(a)) = 1$ or 2. Also, since m is even, from (3.27) and (3.28) $R \mid p_{\frac{1}{2}mR}(a)$. Thus we must have either

$$p_{\frac{1}{2}mR}(a) = 2RY_1^2 \ ; \ q_{\frac{1}{2}mR}(a) = Y_2^2$$

where from theorem 3.1 since $R > 1$ the second equation has no

solution,

or

$$p_{\frac{1}{2}mR}(a) = RY_1^2 \; ; \; q_{\frac{1}{2}mR}(a) = 2Y_2^2$$

From theorem 3.2 the second equation requires $\frac{1}{2}mR = 0$ which gives the stated result.

(ii) Suppose that m is odd. Then $p_n(a) \neq 2RY^2$ except possibly for $m = 1$, $R = 3$. For, except in this case, from parts (ii) and (iii) of the proof of theorem 3.13 we see that for each n there exists k where $2|k$, $3\nmid k$, such that

$$(Rp_n(a) \; / \; q_k(a)) = -1.$$

From (3.17) therefore

$$(2Rp_n(a) \; / \; q_k(a)) = -1$$

Thus $p_n(a) \neq 2RY^2$.

This completes the proof.

We have now proved all the preliminary results we require in order to solve the equations $p_n(a) = NY^2$, $q_n(a) = NX^2$ for a general square-free value of N. We begin the final part of this chapter by proving that in general these equations have at most one solution. Since $p_{-n}(a) = -p_n(a)$ and $q_{-n}(a) = q_n(a)$ we consider only positive values of n. We prove:

THEOREM 3.15. The equations

$$\left.\begin{array}{ll} 1. & p_r(a) = NY_1^2 \\ 2. & p_s(a) = 2NY_2^2 \\ 3. & q_t(a) = NX_1^2 \\ 4. & q_u(a) = 2NX_2^2 \end{array}\right\} \text{where r,s,t, and u are positive}$$

integers, have at most one solution between them for any given odd

square-free integer $N \geqslant 3$. If one of the four equations has a solution there are no solutions of the other three except in the cases:

(i) $a = NK^2$, N square-free, when

$$p_2(a) = NK^2$$
$$q_{\pm 1}(a) = NK^2$$

(ii) $a = K^2$, $a^2 - 2 = NH^2$, N square-free, when

$$p_4(a) = N.(KH)^2$$
$$q_2(a) = NH^2$$

(iii) $a = \frac{1}{2}Q_{2n}(2)$, $a^2 - 1 = 2K^2$, $a(a^2 - 3) = NH^2$, N square-free, when

$$p_6(a) = 2N.(KH)^2$$
$$q_3(a) = N.H^2$$

Proof. If $p_r(a) = NY_1^2$, has two solutions, $r = n$ and $r = m$, then $p_m(a)\, p_n(a) = NY_1^2 . NY'^2_1 = K^2$, say, which is impossible from corollary 3.2.

The other parts of the proof follow in a similar manner from corollary 3.2.

Thus, in general, the equations 1 - 4 of theorem 3.15 have at most one solution between them. We now proceed to the problem of determining this solution if it exists. It is convenient to distinguish, as in theorem 3.15, between an odd square-free integer, and an even one. Thus, from now on, N will denote a positive odd square-free integer.

We need first to consider when a given N will divide $p_n(a)$ or $q_n(a)$.

Let h_r be the least non-negative residue of $p_r(a)$ modulo R, where R is any integer. Since there are only R residues modulo R, there are only R^2 possibilities for the pair of integers (h_r, h_{r+1}). Hence there exist integers m and n such that $h_m = h_n$, and $h_{m+1} = h_{n+1}$ and $m \neq n$. But then, since $p_r(a)$ satisfies a three-term recurrence relation

$$h_{m+t} = h_{n+t}$$

for all integers t. In particular

$$0 = h_0 = h_{m-m} = h_{m-n}$$

i.e. $R \mid p_{m-n}(a)$.

Thus any integer R will divide $p_r(a)$ for some $r \neq 0$. It is not necessarily true, however that R divides $q_r(a)$ for some r, e.g. it is easily seen that $3 \nmid q_r(5)$ for any integer r. Hence we make the following definitions.

DEFINITION. The rank of apparition of an integer R with respect to the sequence $p_r(a)$ is the least positive value of r for which $R \mid p_r(a)$.

DEFINITION. If an integer R divides $q_r(a)$ for some value of r, then the rank of apparition of the integer R with respect to the sequence $q_r(a)$ is the least positive value of r for which $R \mid q_r(a)$. If R does not divide $q_r(a)$ for any value of r then the rank of apparition of R with respect to the sequence $q_r(a)$ is not defined.

The following two lemmas are a direct consequence of the definitions.

LEMMA 3.7. If ρ is the rank of apparition of the integer R with respect to the sequence $p_r(a)$ then $R \mid p_r(a)$ if and only if $\rho \mid n$.

Proof. From lemma 3.1, clearly, if $\rho \mid n$ then $R \mid p_n(a)$ Suppose now that $R \mid p_n(a)$. Then $R \mid (p_n(a), p_\rho(a))$, i.e. $R \mid p_{(n,\rho)}(a)$ by lemma 3.4. Thus, from the definition of ρ, $(n,\rho) \geq \rho$. But clearly $(n,\rho) \leq \rho$. Thus $(n,\rho) = \rho$, i.e. $\rho \mid n$.

LEMMA 3.8. If $R > 2$ is an integer such that the rank of apparition, ρ, of R with respect to the sequence $q_r(a)$ is defined, then $R \mid q_n(a)$ if and only if n is an odd multiple of ρ.

Proof. From lemma 3.2, clearly, if n is odd multiple of ρ then $R \mid q_n(a)$. Suppose now that $R \mid q_n(a)$. Then $R \mid (q_n(a), q_\rho(a))$ where, from lemma 3.5, since $R > 2$, therefore $(q_n(a), q_\rho(a)) = q_{(n,\rho)}(a)$. But then, as in lemma 3.7 we see that $(n,\rho) = \rho$ i.e. $\rho \mid n$. But from lemma 3.5, since $(q_n(a), q_\rho(a)) = q_{(n,\rho)}(a)$ $\frac{n}{(n,\rho)} = \frac{n}{\rho}$ must be odd, i.e. n is an odd multiple of ρ.

We can now proceed to the main results, which are contained in the final four theorems, theorems 3.16 - 3.19.

THEOREM 3.16. Now let N be a positive odd square-free integer whose rank of apparition, ρ, with respect to the sequence $q_r(a)$ is defined. Then

(a) If $3 \nmid \rho$, $q_n(a) = NX^2$ can occur only if $n = \pm\rho$.

(b) If $3 \mid \rho$, $q_n(a) = NX^2$ has no solutions.

Proof. We see first from lemma 3.8 that if $q_n(a) = NX^2$ then $n = r\rho$, where r is an odd integer.

(a) (i) Suppose that $3 \nmid \rho$, $3 \mid r$. Then from (3.9) and (3.10) we see that

$$q_n(a) = q_{\frac{1}{3}r\rho}(a)\,(q_{\frac{1}{3}r\rho}(a)^2 - 3)$$

where, from lemma 3.8, since $3 \mid r$, $N \mid q_{\frac{1}{3}r\rho}(a)$. Also, clearly, $(q_{\frac{1}{3}r\rho}(a),\ q_{\frac{1}{3}r\rho}(a)^2 - 3)$ is 1 or 3 and so, if $q_n(a) = NX^2$ we require either

$$q_{\frac{1}{3}r\rho}(a)^2 - 3 = X_1^2$$

which is impossible since $r \neq 0$, or

$$q_{\frac{1}{3}r\rho}(a)^2 - 3 = 3X_1^2$$

which is impossible modulo 9.

(ii) Suppose now that $3 \nmid \rho$, $3 \nmid r$. Then $q_n(a) \neq NX^2$ except possibly for $r = \pm 1$. For, if $q_\rho(a) = NX^2$, $q_{r\rho}(a) \neq NX^2$ for any $r \neq \pm 1$, by theorem 3.15. If $q_\rho(a) \neq NX^2$ then $q_\rho(a) = N.Rx^2$ for some square-free integer R. Since $3 \nmid r\rho$, from (3.13) Rx is odd.

Now since $2 \nmid r$, $3 \nmid r$, $r \equiv \pm 1 \pmod 6$ and so, from (3.16) and (3.7)

$$q_{r\rho}(a) \equiv q_\rho(a) \pmod 8.$$

Thus, since N is odd, if $q_{r\rho}(a) = NX^2$

$$X^2 \equiv Rx^2 \pmod 8$$

i.e. $R \equiv 1 \pmod 8$. We therefore suppose that $R \equiv 1 \pmod 8$. Now from (3.36) $q_{r\rho}(a) = q_r(q_\rho(a))$, and since $3 \nmid \rho$, from (3.13), $q_\rho(a)$ is odd. If $r \neq \pm 1$, we may write $r = \pm 1 + 2.3^s.k$ where $2 \mid k$, $3 \nmid k$. Repeated applications of (3.23) now give

$$q_r(q_\rho(a)) \equiv -q_{\pm 1}(q_\rho(a)) \pmod{q_k(q_\rho(a))}$$

$$\equiv -q_\rho(a) \pmod{q_k(q_\rho(a))}$$

Hence,

$$(Nq_{r\rho}(a) \,/\, q_k(q_\rho(a))) = (-N.NRx^2 \,/\, q_k(q_\rho(a)))$$
$$= -(R \,/\, q_k(q_\rho(a))) \text{ by (3.17)}$$
$$= -(q_k(q_\rho(a)) \,/\, R) \text{ since } R \equiv 1 \pmod 8$$
$$= -(2 \,/\, R) \text{ by (3.34) since } R \mid q_\rho(a)$$
$$= -1 \text{ since } R \equiv 1 \pmod 8$$

Thus $q_{r\rho}(a) \neq NX^2$ except possibly for $r = \pm 1$.

This completes the proof of (a).

(b) From (3.16) and the first six values of $q_r(a)$, if $3 \mid r\rho$, $q_{r\rho}(a) \equiv 2 \pmod 8$. Thus if N is odd, $q_{r\rho}(a) \neq NX^2$.

This completes the proof of the theorem.

THEOREM 3.17. Let N be a positive odd square-free integer whose rank apparition, ρ, with respect to the sequence $q_n(a)$ is defined. Then $q_n(a) = 2NX^2$ can occur only if $n = \pm\rho$.

Proof. From lemma 3.8 we note first that if $q_n(a) = 2NX^2$ then $n = r\rho$ where r is an odd integer.

(i) Suppose that $3 \mid r$. Then from (3.9) and (3.10) again

$$q_n(a) = q_{\frac{1}{3}r\rho}(a)\,(q_{\frac{1}{3}r\rho}(a)^2 - 3)$$

where $N \mid q_{\frac{1}{3}r\rho}(a)$ and $(q_{\frac{1}{3}r\rho}(a), q_{\frac{1}{3}\rho}(a)^2 - 3) = 1$ or 3. Thus if $q_n(a) = 2NX^2$ we require either

$$q_{\frac{1}{3}r\rho}(a)^2 - 3 = X_1^2 \text{ or } 3X_1^2$$

which as in the proof of theorem 3.16 is impossible, or

$$q_{\frac{1}{3}r\rho}(a)^2 - 3 = 2X_1^2$$

which is impossible modulo 8, or

$$q_{\frac{1}{3}r\rho}(a)^2 - 3 = 6X_1^2.$$

Since $3 \mid a = p_2(a)$ or $3 \mid a^2 - 1 = p_3(a)$, from lemma 3.6 this last case holds only if $3 \mid a$ and $\frac{1}{3}r\rho$ is odd. If these conditions

hold, from (3.11) we have

$$6X_1^2 + 1 = q_{3^r\rho}(a)$$

where $3^r\rho = \pm 2 + 2.3^s.k$ where $4 \nmid k$, $3 \nmid k$. Repeated applications of (3.23) now give

$$6X_1^2 + 1 \equiv -(a^2 - 2) \pmod{q_k(a)}$$

or

$$6X_1^2 \equiv -(a^2 - 1) \pmod{q_k(a)}$$

It is easily shown by induction that since $4 \nmid k$ $q_k(a) \equiv 2 \pmod 3$, and so, if $a^2 - 1 = 2^s.c$ where c is odd,

$$(6 / q_k(a)) = (-2^s.c / q_k(a))$$

or

$$(3 / q_k(a)) = (-c / q_k(a)) \text{ by (3.17)}$$

Thus, again by (3.17) we have

$$1 = -(q_k(a) / 3) = -(-q_k(a) / c)$$

But now $a^2 - 1 = 2^s.c = p_3(a)$ and so from (3.21) since $k \equiv \pm 2 \pmod 6$

$$1 = -(-(a^2 - 2) / c) = -(1 / c) = -1$$

which is impossible. Thus $q_{3^r\rho}(a) \neq 6X_1^2 + 1$ and we cannot have $3 \mid r$.

(ii) Suppose now that $3 \nmid r$. Then clearly from (3.13), if $q_n(a) = 2NX^2$ $3 \mid \rho$. Then, from (3.9) and (3.10) we have

$$q_n(a) = q_{3^r\rho}(a)\,(q_{3^r\rho}(a)^2 - 3)$$

for all integers r. In particular, since $3|\rho$, $2N \Big| \left(q_{\frac{1}{3}\rho}(a) \times (q_{\frac{1}{3}\rho}(a)^2 - 3)\right)$. Let $2N = N_1 N_2$ where $N_1 | q_{\frac{1}{3}\rho}(a)$, $N_2 | q_{\frac{1}{3}\rho}(a)^2 - 3$ and if $3|2N$ let $3|N_2$. Now from lemma 3.2 $N_1 | q_{\frac{1}{3}\rho r}(a)$ and since $3 \nmid r$, by lemma 3.5 $(q_\rho(a), q_{\frac{1}{3}r\rho}(a)) = q_{\frac{1}{3}\rho}(a)$. Hence $N_2 | q_{\frac{1}{3}r\rho}(a)^2 - 3$ and if $q_{r\rho}(a) = 2NX^2$ we require

$$q_{\frac{1}{3}\rho r}(a) = N_1 X_1^2 \text{ or } 3N_1 X_1^2 .$$

Now if $3 | q_{\frac{1}{3}r\rho}(a)$ it is easily seen from (3.12) that $3|a = q_1(a)$. Thus, from lemma 3.2 $\frac{1}{3}\rho r$ is odd and $3 | q_{\frac{1}{3}\rho}(a)$. In either case, therefore, we require

$$q_{\frac{1}{3}r\rho}(a) = MX_1^2$$

where $M | q_{\frac{1}{3}\rho}(a)$. If $M = 1$, form theorem 3.1, $\frac{1}{3}\rho r = \pm 1$, i.e. $r = \pm 1$. If $M = 2$, from theorem 3.2, there are no solutions since $N > 1$.

If $M > 1$ and M is odd, from theorem 3.16 again $r = \pm 1$, whereas if $M > 2$ and M is even from the above either $r = \pm 1$ or $3 | \frac{1}{3}\rho r$. If $3 | \frac{1}{3}\rho r$ we repeat the above process until all factors of 3 in ρ are exhausted when again we see that $r = \pm 1$ is the only possibility.

This completes the proof.

THEOREM 3.18. Let N_1 be a positive odd square-free integer such that the rank of apparition, ρ_1 of N_1 with respect to the sequence $q_r(a)$ is defined and let N_2 be a positive odd square-free integer such that $(N_2, q_n(a)) = 1$ for all integers n. Let the rank of apparition of N_2 with respect to the sequence $p_r(a)$ be ρ_2. Then ρ_2 is odd and

(a) $p_n(a) = N_1 Y^2$ can occur only if $(n = 0)$, $(a = N_1 Y^2, n = 2)$, $(a = \frac{1}{2}Q_{2n}(2), a^3 - 3a = 2N_1 Y_1^2, n = 6)$ or $(a = Y_1^2, a^2 - 2 = N_1 Y_2^2, n = 4)$

(b) $p_n(a) = 2N_1Y^2$ can occur only if $n = 0$.

(c) $p_n(a) = N_2Y^2$ can occur only if $(n = 0)$ or $(n = \rho_2)$.

(d) $p_n(a) = 2N_2Y^2$ can occur only if $(n = 0)$ or $(n = \rho_2, 3|\rho_2)$.

Proof. We show first that ρ_2 is odd. For if $\rho_2 = 2\rho$, then from (3.9)

$$p_{\rho_2}(a) = p_\rho(a)\ q_\rho(a)$$

where, since $(N_2, q_\rho(a)) = 1$, $N_2 | p_\rho(a)$. But $\rho < \rho_2$ and this contradicts the definition of ρ_2. Thus ρ_2 is odd.

(a) Suppose first that $p_n(a) = N_1Y^2$. Then since $N_1 | q_{\rho_1}(a)$, $N_1 | (q_{\rho_1}(a), p_n(a))$ where $N_1 > 2$. From lemma 3.6 therefore $N_1 | q_{(n,\rho_1)}(a)$ and $\frac{n}{(n,\rho_1)}$ is even. But since ρ_1 is the rank apparition of N_1 with respect to the sequence $q_r(a)$, therefore $(n,\rho_1) = \rho_1$ and so $n = 2r\rho_1$ for some integer r.
Then from (3.9)

$$N_1Y^2 = p_{r\rho_1}(a)\ \ q_{r\rho_1}(a)$$

If r is even, from lemma 3.1 and (3.9)
$N_1 | p_{2\rho_1}(a) = p_{\rho_1}(a)\ q_{\rho_1}(a)$. Also $p_{2\rho_1}(a) \mid p_{r\rho_1}(a)$. Thus we require

$$q_{r\rho_1}(a) = X_1^2 \text{ or } 2X_1^2$$

which from theorems 3.1 and 3.2 implies $n = 0$ since r is even.
If r is odd, from lemma 3.2 $N_1 | q_{r\rho_1}(a)$ and so we require

$$p_{r\rho_1}(a) = Y_1^2 \text{ or } 2Y_1^2$$

From theorems 3.3. and 3.4 we now see that $p_n(a) = N_1Y^2$ only in the cases stated.

(b) Suppose now that $p_n(a) = 2N_1Y^2$. Then as above we find that $n = 2r\rho_1$ for some integer r. Thus from (3.9)

$$2N_1Y^2 = p_{r\rho_1}(a)\ q_{r\rho_1}(a)$$

where from (3.13), $3 \mid r\rho_1$.

As in (a) again we find that if r is even $N_1 \mid p_{r\rho_1}(a)$ and we require

$$q_{r\rho_1}(a) = X_1^2 \text{ or } 2X_1^2$$

which is possible, since r is even, from theorem 3.1 and 3.2, only for $n = 0$.

If r is odd again we find $N_1 \mid q_{r\rho_1}(a)$ and we require

$$p_{r\rho_1}(a) = Y_1^2 \text{ or } 2Y_1^2$$

which is possible, since $3 \mid r\rho_1$, from theorems 3.3 and 3.4 only for $r\rho_1 = 3$, but this gives no result.

(c) Suppose now that $p_n(a) = N_2Y^2$. Then clearly, from lemma, 3.7, $n = r\rho_2$ for some integer r.

(i) Suppose that r is even. Let $r = 2r'$. Then from (3.9)

$$N_2Y^2 = p_{r'\rho_2}(a)\ q_{r'\rho_2}(a)$$

where $N_2 \mid p_{r'\rho_2}(a)$ by lemma 3.7. From (3.14), $(p_{r'\rho_2}(a),\ q_{r'\rho_2}(a)) = 1$ or 2. Thus we require

$$q_{r'\rho_2}(a) = X_1^2 \text{ or } 2X_1^2$$

From theorems 3.1 and 3.2 we now find that the only result is $(n = 0)$.

(ii) Suppose now that r is odd. Then $3 \nmid r$. For if $r = 3r'$, from (3.9) and (3.10)

$$N_2 Y^2 = p_{r'\rho_2}(a)\,(q_{r'\rho_2}(a)^2 - 1)$$

where, from (3.12), $(p_{r'\rho_2}(a),\ q_{r'\rho_2}(a)^2 - 1) = 1$ or 3. Also, by lemma 3.7, $N \mid p_{r'\rho_2}(a)$. Thus if $p_n(a) = N_2 Y^2$ we require either

$$q_{r'\rho_2}(a)^2 - 1 = Y_1^2$$

which is impossible since $|q_{\rho_2}(a)| > 1$, or

$$q_{r'\rho_2}(a)^2 - 1 = 3Y_1^2,\quad p_{r'\rho_2}(a) = 3Y_2^2.$$

Since $3 \mid a = p_2(a)$ or $3 \mid a^2 - 1 = p_3(a)$ and $r'\rho_2$ is odd, by lemma 3.1 from the second equation $3 \mid a^{2^3} - 1$, $3 \nmid a$. But then the first equation is impossible from (3.34). Thus $3 \nmid r$.

(iii) Suppose now that $2 \nmid r$, $3 \nmid r$ and $3 \nmid \rho_2$. Then $p_n(a) = N_2 Y^2$ can occur only if $r = 1$. For if $p_{\rho_2}(a) = N_2 Y^2$, $p_{r\rho_2}(a) \neq N_2 Y^2$ for any $r \neq 1$ by theorem 3.15. If $p_{\rho_2}(a) \neq N_2 Y^2$ then $p_{\rho_2}(a) = N_2 \cdot R y^2$ for some square-free integer R where since $3 \nmid r\rho_2$ from (3.13) R is odd. Then from (3.35),

$$p_{r\rho_2}(a) = p_{\rho_2}(a)\ p_r\left(q_{\rho_2}(a)\right)$$

where, since $3 \nmid \rho_2$, $q_{\rho_2}(a)$ is odd by (3.13). Then, if $p_n(a) = N_2 Y^2$, we require $p_r\left(q_{\rho_2}(a)\right) = RY_1^2$ where $R \mid q_{\rho_2}(a)^2 - 4$ from (3.12). From (3.13) $q_{\rho_2}(a)$ is odd, and so from theorem 3.13 we see that since we are considering the case $2 \nmid r$, $3 \nmid r$, there are no solutions of this equation. Thus the only possibility here is $r = 1$.

(iv) Suppose finally that $2 \nmid r$, $3 \nmid r$ but $3 \mid \rho_2$. Here again we

can have only r = 1. For, from (3.9) and (3.10) we have

$$p_{r\rho_2}(a) = p_{\frac{1}{3}r\rho_2}(a) \quad (q_{\frac{1}{3}r\rho_2}(a)^2 - 1)$$

for all integers r. In particular, $N_2 \mid p\rho_2(a) = p_{\frac{1}{3}\rho_2}(a) \times (q_{\frac{1}{3}\rho_2}(a)^2 - 1)$. Let $N_2 = M_1 M_2$ where $M_1 \mid p_{\frac{1}{3}\rho_2}(a), M_2 \mid q_{\frac{1}{3}\rho_2}(a)^2 - 1$ and if $3 \mid N_2$ let $3 \mid M_2$. Then from lemma 3.1 clearly $M_1 \mid p_{\frac{1}{3}r\rho_2}(a)$ and from lemma 3.4, since $3 \nmid r$, $(p\rho_2(a), p_{\frac{1}{3}r\rho_2}(a)) = p_{\frac{1}{3}\rho_2}(a)$. Thus $M_2 \mid q_{\frac{1}{3}r\rho_2}(a)^2 - 1$. Hence, if $p_n(a) = N_2 Y^2$ we require either

$$p_{\frac{1}{3}\rho_2 r}(a) = M_1 Y_1^2 \; ; \quad q_{\frac{1}{3}\rho_2 r}(a)^2 - 1 = M_2 Y_2^2$$

or

$$p_{\frac{1}{3}\rho_2 r}(a) = 3M_1 Y_1^2 \; ; \quad q_{\frac{1}{3}\rho_2 r}(a)^2 - 1 = 3M_2 Y_2^2$$

since from (3.12) $(p_{\frac{1}{3}\rho_2 r}(a), q_{\frac{1}{3}\rho_2 r}(a)^2 - 1) = 1$ or 3. But again, either $3 \mid a = p_2(a)$ or $3 \mid a^2 - 1 = p_3(a)$ and so from lemma 3.7 either $3 \mid \frac{1}{3}r\rho_2$ or $2 \mid \frac{1}{3}r\rho_2$. But since $2 \nmid r$, $3 \nmid r$ therefore clearly, $3 \mid p_{\frac{1}{3}\rho_2 r}(a)$ implies $3 \mid p_{\frac{1}{3}\rho_2}(a)$.
Thus in either case we require,

$$p_{\frac{1}{3}\rho_2 r}(a) = M_3 Y_3^2$$

where $M_3 \mid p_{\frac{1}{3}\rho_2}(a)$. If $M_3 = 1$, from theorem 3.1 $\frac{1}{3}r\rho_2 = 1$ whence $r = 1$. If $M_3 > 1$, from the above, if $3 \nmid \frac{1}{3}\rho_2 r$, $r = 1$. If $3 \mid \frac{1}{3}\rho_2 r$ we have the same situation as that we started with and may repeat the above process until all the factors of 3 in ρ_2 are exhausted. Thus eventually we see that the only possibility is $r = 1$.

This completes the proof of (c).

(d) Suppose now that $p_n(a) = 2N_2 Y^2$. Then again from lemma 3.7 we see that $n = r\rho_2$, for some integer r.

(i) Suppose that r is even. Put $r = 2r'$. Then from (3.9)

$$2N_2Y^2 = p_{r'\rho_2}(a)\ q_{r'\rho_2}(a)$$

where by lemma 3.7 $N_2 \mid p_{r'\rho_2}(a)$ and from (3.14) $(p_{r'\rho_2}(a), q_{r'\rho_2}(a)) = 1$ or 2.

Thus we require

$$q_{r'\rho_2}(a) = X_1^2 \text{ or } 2X_1^2$$

From theorems 3.1 and 3.2 the only result is $r = 0$.

Thus if r is even, $r = 0$.

(ii) Suppose now that $2 \nmid r$. We show that $3 \nmid r$. For if $3 \mid r$, from (3.9) and (3.10) we have

$$2N_2Y^2 = p_{\frac{1}{3}r\rho_2}(a)\ (q_{\frac{1}{3}r\rho_2}(a)^2 - 1)$$

where from (3.12) $(p_{\frac{1}{3}r\rho_2}(a), q_{\frac{1}{3}\rho_2 r}(a)^2 - 1) = 1$ or 3. Also, since $3 \mid r$, from lemma 3.7 $N_2 \mid p_{\frac{1}{3}r\rho_2}(a)$. Thus if $p_n(a) = 2N_2Y^2$ we require

$$q_{\frac{1}{3}r\rho_2}(a)^2 - 1 = Y_1^2$$

which is impossible since $\left|q_{\frac{1}{3}r\rho_2}(a)\right| > 1$, or

$$q_{\frac{1}{3}r\rho_2}(a)^2 - 1 = 2Y_2^2$$

where clearly $3 \nmid \frac{1}{3} r\rho_2$ from (3.13) and so since $2 \nmid \frac{1}{3}r\rho_2$ from (3.32) $\frac{1}{3} r\rho_2 = 1$, i.e. $\rho_2 = 1$ which is impossible since $N_2 > 1$, or

$$q_{\frac{1}{3}r\rho_2}(a)^2 - 1 = 3Y_1^2 \ ; \ p_{\frac{1}{3}r\rho_2}(a) = 6Y_2^2$$

or

$$q_{\frac{1}{3}r\rho_2}(a)^2 - 1 = 6Y_1^2 ; \ p_{\frac{1}{3}r\rho_2}(a) = 3Y_2^2$$

In either of these cases as shown in the proof of (c) the second equation requires $3 \mid a^2 - 1$, $3 \nmid a$. But then, in each case, from (3.34) the first equation is impossible. Thus $3 \nmid r$.

(iii) Suppose that $2 \nmid r$, $3 \nmid r$. Then, if $p_n(a) = 2N_2 Y^2$, from (3.13), $3 \mid \rho_2$. From (3.9) and (3.10) again we find

$$p_{r\rho_2}(a) = p_{\frac{1}{3}r\rho_2}(a)\,(q_{\frac{1}{3}r\rho_2}(a)^2 - 1)$$

for all integers r. In particular, again we let $2N_2 = M_1 M_2$ where $M_1 \mid p_{\frac{1}{3}\rho_2}(a)$, $M_2 \mid q_{\frac{1}{3}\rho_2}(a)^2 - 1$ and if $3 \mid N_2$ let $3 \mid M_2$. Then as in the proof of (c) we can show that $M_1 \mid p_{\frac{1}{3}r\rho_2}(a)$, $M_2 \mid q_{\frac{1}{3}r\rho_2}(a)^2 - 1$ and that again we need a solution of an equation of the form

$$p_{\frac{1}{3}r\rho_2}(a) = M_3 Y_3^2$$

where $M_3 \mid p_{\frac{1}{3}\rho_2}(a)$. If $M = 1$ or 2 from theorems 3.3. and 3.4, since $\frac{1}{3}r\rho_2$ is odd the only possibilities are $\frac{1}{3}r\rho_2 = 1$ or 3. Since $3 \nmid r$ therefore, $r = 1$. If $M_3 > 2$ is odd from (c) again $r = 1$ is the only possibility. If $M_3 > 2$ is even we have the situation with which we started and may repeat the above process until all factors of 3 in ρ_2 are exhausted. We must finally arrive at one of the other cases whence again $r = 1$.

This completes the proof of theorem 3.18.

THEOREM 3.19. Let N be a positive odd square-free integer such that $N \nmid q_r(a)$ for any integer r, but $(N, q_s(a)) > 2$ for at least one integer s. Let the rank of apparition of N with respect to the sequence $p_n(a)$ be ρ. Then

(a) $p_n(a) = NY^2$ can occur only if $(n = 0)$, or $(n = \rho)$.

(b) $p_n(a) = 2NY^2$ can occur only if $(n = 0)$ or $(n = \rho)$.

Proof. If $p_n(a) = NY^2$ or $2NY^2$ where $(N, q_s(a)) > 2$, from lemma

3.6 we see that n must be even. If $n = 0$, $p_o(a) = N.0^2$.
If $n \neq 0$, put $n = 2^t.c$ where c is odd, $t \geq 1$. Then from (3.9) we find

$$p_n(a) = p_c(a)\ q_c(a)\ q_{2c}(a)\ \ldots\ q_{2^{t-1}c}(a)$$

where, from lemmas 3.3 and 3.6,

$$(p_c(a),\ q_{2^i c}(a)) \mid 4,\quad (q_{2^i c}(a),\ q_{2^j c}(a)) \mid 2 \text{ where } i \neq j.$$

Since $N \mid p_n(a)$, let

$$N = N_o N_1 N_2 \ldots N_{t-1}$$

where

$$N_o \mid p_c(a),\ N_i \mid q_{2^i c}(a)\ 1 \leq i \leq t-1.$$

Now we see that if $p_n(a) = NY^2$ or $2NY^2$, then we require

$$p_c(a) = N_o Y_o^2 \text{ or } 2N_o Y_o^2$$

and

$$q_{2^i c}(a) = N_i Y_i^2 \text{ or } 2N_i Y_i^2$$

If $N_{t-1} = 1$, from theorems 3.1 and 3.2 we find that there are no solutions of $p_n(a) = NY^2$ or $2NY^2$.
If $N_{t-1} > 1$, from lemma 3.8 we see that the rank of apparition of N with respect to the sequence $q_n(a)$ is of the form $2^{t-1}.\sigma$, where σ is odd. Thus, from lemma 3.6, $\rho = 2^t.c'$, where $\sigma \mid c'$.
From lemma 1.7, now $c' \mid c$. Since we require $q_{2^{t-1}c}(a)$ $= N_{t-1} Y_{t-1}^2$ or $2N_{t-1} Y_{t-1}^2$, therefore, from theorems 3.16 and

3.17 we must have $\sigma = c' = c$.

This completes the proof of theorem 3.19 and concludes this chapter.

CHAPTER 4.

In this chapter we suppose that the equation $X^2 - dY^2 = -4$ has no solutions and that the equation $X^2 - dY^2 = 4$ has only solutions (X,Y) for which X and Y are both even.

As in the previous chapter, we seek solutions of the equation $X^4 - dY^2 = 1,4$ and $X^2 - dY^4 = 1,4$ among the solutions of the equations $X^2 - dY^2 = 1,4$ but as in chapter 2 the method gives only very limited results.

We begin once again by establishing some results concerning the solutions of the equations $X^2 - dY^2 = 1,4$ which are very similar to those obtained at the beginning of chapter 3.

Clearly, since we are supposing that all solutions of $X^2 - dY^2 = 4$ are even, the fundamental solution (A,B) is even, i.e. A and B are both even. We put A = 2a and B = 2b. The general solution of $X^2 - dY^2 = 4$ is now given in terms of a and b by

$$X + Yd^{\frac{1}{2}} = 2\left(\frac{2a + 2bd^{\frac{1}{2}}}{2}\right)^n = 2(a + bd^{\frac{1}{2}})^n$$

As before we write $\alpha = a + bd^{\frac{1}{2}}$ and $\beta = a - bd^{\frac{1}{2}}$ and have

$$\alpha + \beta = 2a; \quad \alpha\beta = 1 \tag{4.1}$$

As in chapter 3, we define, for all integers n,

$$p_n(2a) = \frac{1}{2bd^{\frac{1}{2}}}(\alpha^n - \beta^n) \tag{4.2}$$

$$q_n(2a) = \alpha^n + \beta^n \tag{4.3}$$

and obtain, exactly as before,

$$p_{n+2}(2a) = 2ap_{n+1}(2a) - p_n(2a) \tag{4.4}$$

$$q_{n+2}(2a) = 2aq_{n+1}(2a) - q_n(2a) \tag{4.5}$$

$$p_{-n}(2a) = -p_n(2a) \tag{4.6}$$

$$q_{-n}(2a) = q_n(2a) \tag{4.7}$$

Also, $p_0(2a) = 0$, $p_1(2a) = 1$, $q_0(2a) = 2$ and $q_1(2a) = 2a$. Thus it is clear that $p_n(2a)$ and $q_n(2a)$ are integers for all integers n and moreover positive for positive n. The first few values are:

n	$p_n(2a)$	$q_n(2a)$
0	0	2
1	1	2a
2	2a	$4a^2 - 2$
3	$4a^2 - 1$	$8a^3 - 6a$
4	$8a^3 - 4a$	$16a^4 - 16a^2 + 2$
5	$16a^4 - 12a^2 + 1$	$32a^5 - 40a^3 + 10a$
6	$32a^5 - 32a^3 + 6a$	$64a^6 - 96a^4 + 36a^2 - 2$

Again as in chapter 3 we obtain

$$2p_{m+n}(2a) = p_m(2a)\, q_n(2a) + q_m(2a)\, p_n(2a) \tag{4.8}$$

$$2q_{m+n}(2a) = (4a^2 - 4)p_n(2a)p_m(2a) + q_n(2a)q_m(2a) \tag{4.9}$$

$$q_n(2a)^2 = q_{2n}(2a) + 2 \tag{4.10}$$

$$q_n(2a)^2 = (4a^2 - 4)p_n(2a)^2 + 4 \tag{4.11}$$

and from (4.8) - (4.11)

$$q_{m+2N}(2a) \equiv -q_m(2a) \pmod{q_N(2a)} \tag{4.12}$$

Now if $2a = 2^h a'$ where a' is odd then clearly 2^h is the highest power of 2 which divides $q_1(2a) = 2a$. But from (4.5)

$$q_{2n+1}(2a) = 2aq_{2n}(2a) - q_{2n-1}(2a)$$

and, by virtue of (4.7), a simple inductive arguement shows that

if $2a = 2^h.a'$ where a' is odd, then $q_{2n+1}(2a) = 2^h.K$ for some odd integer K (4.13)

From (4.10)

$$q_{2n}(2a) = q_n(2a)^2 - 2$$

and since $2 \mid q_n(2a)$ therefore

$$q_{2n}(2a) \equiv 2 \pmod 4 \qquad (4.14)$$

From (4.8), $p_{2n}(2a) = p_n(2a)q_n(2a)$ and therefore, from the above, $p_{2n}(2a)$ is even. Clearly $p_1(2a) = 1$ is odd. Also from (4.4)

$$p_{2n+1}(2a) = 2ap_{2n}(2a) - p_{2n-1}(2a)$$

and so, by induction, with (4.6), we have

$$2 \mid p_{2n}(2a) \; ; \; p_{2n+1}(2a) \text{ is odd} \qquad (4.15)$$

Now from (4.9) we find

$$\begin{aligned} 2q_{m+s}(2a) &= (4a^2 - 4)p_m(2a)p_s(2a) + q_m(2a)q_s(2a) \\ &= (4a^2 - 4)\left(p_m(2a)p_4(2a)q_4(2a) + p_4(2a)^2 q_m(2a)\right) \\ &\quad + 2\,q_m(2a) \text{ by (4.8), (4.10) and (4.11)} \\ &\equiv 2q_m(2a) \pmod{2(4a^2 - 4)p_4(2a)} \\ &\quad \text{since } p_4(2a) \text{ and } q_4(2a) \text{ are even.} \end{aligned}$$

Now $p_4(2a) = 2a(4a^2 - 2)$ and so if $2a = 2^h a'$ where a' is odd, $2^{h+1} \mid p_4(2a)$.

Thus clearly

$$q_{m+8}(2a) \equiv q_m(2a) \pmod{8.2^h}$$

Thus from (4.13) and (4.14) we have

$$\text{if } m \text{ is odd and } 2^h \mid 2a \text{ then } \tfrac{1}{2}hq_{m+8}(2a) \equiv \tfrac{1}{2}hq_m(2a) \pmod 8 \tag{4.16}$$

$$\text{if } m \text{ is even and } 2^h \mid 2a \text{ then } \tfrac{1}{2}q_{\frac{m}{2}+8}(2a) \equiv \tfrac{1}{2}q_m(2a) \pmod{2^{h+\frac{m}{2}}} \tag{4.17}$$

It will be readily seen that the proofs of lemmas 3.1 - 3.6 do not depend in any essential way upon the fact that a is odd. Hence the results carry over to the present case. We need only one of these results which for the sake of completeness we prove here.

LEMMA 4.1. $p_n(2a) \mid p_{tn}(2a)$ for all integers t.

Proof. From (4.6) we see that we need only consider $t \geqslant 0$ and hence we use proof by induction. The result is clearly true for $t = 1$. Assume it true for $t \leqslant r - 1$. Then from (4.8)

$$2p_{nr}(2a) = p_{(r-1)n}(2a)q_n(2a) + q_{(r-1)n}(2a)p_n(2a)$$

where from (4.13) and (4.14) clearly $2p_n(2a)$ divides the right hand side of the equation. Thus $p_n(2a) \mid p_{nr}(2a)$ and the result is true by induction.

Finally we observe that if $2\alpha = 2a + 2bd^{\frac{1}{2}}$ is the fundamental solution of $X^2 - dY^2 = 4$ then the fundamental solution of $X^2 - dY^2 = 1$ is α. Hence the general solution of $X^2 - dY^2 = 4$ is $X = q_n(2a)$, $Y = 2bp_n(2a)$

(IV.I)

the general solution of $X^2 - dY^2 = 1$ is $X = \frac{1}{2}q_n(2a)$, $Y = bp_n(2a)$

(IV.II.)

We are seeking solutions of the equations $X^4 - dY^2 = 1,4$ and $X^2 - dY^4 = 1,4$. Clearly the solutions of $X^4 - dY^2 = 4$ are given by $X^2 = q_n(2a)$, $Y = 2bp_n(2a)$ with similar results for the other equations. We would therefore like to prove results which would enable us to say when $p_n(2a) = Y^2$, $2Y^2$ and $q_n(2a) = X^2$, $2X^2$. However, even in the limited case when we restrict a to being even it is not possible to give results covering all these cases. The results which have been obtained are contained in the following three theorems.

THEOREM 4.1. a) The equation $q_{2n}(2a) = X^2$ has no solutions.

b) If $2a = 2^t.a'$ where a' is odd and $t \geqslant 3$ is odd, then the equation $q_{2n+1}(2a) = X^2$ has no solutions.

c) If $2a = 2^t.a'$ where $t \geqslant 2$ is even and $a' \equiv -1 \pmod 4$ or $a' \equiv 5 \pmod 8$ then the equation $q_{2n+1}(2a) = X^2$ has no solutions.

Proof. a) From (4.14) $2 \mid q_{2n}(2a)$, $4 \nmid q_{2n}(2a)$ and hence $q_{2n}(2a) \neq X^2$.

b) From (4.13) $q_{2n+1}(2a) = 2^t.K$ where K is an odd integer and so if t is odd $q_{2n+1}(2a) \neq X^2$.

c) From (4.13) $q_{2n+1}(2a) = 2^t.K$ where K is odd and so if $q_{2n+1}(2a) = X^2$ $\frac{1}{2^t}q_{2n+1}(2a) = X_1^2$ where X_1 is odd. From (4.16) therefore we require either

$$2n + 1 \equiv \pm 1 \pmod 8, \quad X_1^2 \equiv a' \pmod 8$$

which is impossible if $a' \equiv -1 \pmod 4$ or $a' \equiv 5 \pmod 8$, or

$$2n + 1 \equiv \pm 3 \pmod 8, \quad X_1^2 \equiv a'(4a^2 - 3) \equiv 5a' \pmod 8$$

which is impossible if $a' \equiv -1 \pmod 4$.

Suppose therefore that $2n + 1 \equiv \pm 3 \pmod 8$ and $a' \equiv 5 \pmod 8$. Then from (4.12), putting $2n + 1 = 4m \pm 1$ where m is odd,

$$q_{2n+1}(2a) \equiv -q_{\pm 1}(2a) \pmod{q_{2m}(2a)}$$

Since m is odd from lemma 4.1 $q_2(2a) \mid q_{2m}(2a)$ and so, by virtue of (4.7),

$$q_{2n+1}(2a) \equiv -2a \pmod{4a^2 - 2}$$

Thus

$$\begin{aligned}(q_{2n+1}(2a) \,/\, 2a^2 - 1) &= (-2a \,/\, 2a^2 - 1) \\ &= (-a' \,/\, 2a^2 - 1) \\ &= -(a' \,/\, 2a^2 - 1) \text{ since a is even} \\ &= -(2a^2 - 1 \,/\, a') \text{ since } a' \equiv 5 \pmod 8 \\ &= -1 \text{ since } a' \equiv 5 \pmod 8\end{aligned}$$

Thus $q_{2n+1}(2a) \neq X^2$.

This completes the proof.

THEOREM 4.2. a) If $4 \mid 2a$ then the equation $q_{2n}(2a) = 2X^2$ has only the solution $n = 0$.

b) If $2a = 2^t.a'$ where a' is odd and $t \geqslant 2$ is even, then the equation $q_{2n+1}(2a) = 2X^2$ has no solutions.

c) If $2a = 2^t.a'$ where $t \geqslant 3$ i odd and $a' \equiv -1 \pmod 4$ or $a' \equiv 5 \pmod 8$ then the equation $q_{2n+1}(2a) = 2X^2$ has no solutions.

Proof. a) (i) If $2n \equiv 2 \pmod 4$ then $q_{2n}(2a) \neq 2X^2$. For, from (4.16)

$$\begin{aligned}\tfrac{1}{2}q_{2n}(2a) &\equiv \tfrac{1}{2}(4a^2 - 2) \pmod 8 \\ &\equiv -1 \pmod 8\end{aligned}$$

since $2 \mid a$. Thus $q_{2n}(2a) \neq 2X^2$.

(ii) If $4 \mid n$ then $q_{2n}(2a) \neq 2X^2$ except for $n = 0$. For suppose first that $3 \nmid n$. Then $2n = 6m \pm 2$ where m is odd. From (4.12) now we find

$$q_{2n}(2a) \equiv -q_{\pm 2}(2a) \pmod{q_{3m}(2a)}$$

where from lemma 4.1, since m is odd, $q_3(2a) \mid q_{3m}(2a)$ Thus, by virtue of (4.7)

$$q_{2n}(2a) \equiv -(4a^2 - 2) \pmod{4a^2 - 3}$$

and so

$$\begin{aligned}(2q_{2n}(2a) \,/\, 4a^2 - 3) &= (-2(4a^2 - 2) \,/\, 4a^2 - 3) \\ &= (-2 \,/\, 4a^2 - 3) \\ &= -1 \text{ since a is even and so } 4a^2 - 3 \\ &\equiv 5 \pmod 8\end{aligned}$$

Thus $q_{2n}(2a) \neq 2X^2$.

If $3 \mid n$ from (4.9), (4.8) and (4.10) we find that

$$q_{2n}(2a) = q_{\frac{2n}{3}}(2a)\,(q_{\frac{2n}{3}}(2a)^2 - 3)$$

where clearly $(q_{\frac{2n}{3}}(2a),\ q_{\frac{2n}{3}}(2a)^2 - 3) = 1$ or 3. If $q_{2n}(2a) = 2X^2$, therefore we require

$$q_{\frac{2n}{3}}(2a)^2 - 3 = X_1^2$$

which implies $n = 0$, or

$$q_{\frac{2n}{3}}(2a)^2 - 3 = 3X_1^2$$

which is impossible modulo 9.

This completes the proof of a).

b) From (4.13) $q_{2n+1}(2a) = 2^t.K$ where K is odd, and so if t is even, $q_{2n+1}(2a) \neq 2X^2$.

c) From (4.13) $q_{2n+1}(2a) = 2^t.K$ where K is odd and so if

$q_{2n+1}(2a) = 2X^2$, $\frac{1}{2}t q_{2n+1}(2a) = X_1^2$ where X_1 is odd but as in the proof of theorem 4.1 part c) this is impossible if $a' \equiv -1 \pmod 4$ or $a' \equiv 5 \pmod 8$.

This completes the proof.

THEOREM 4.3. a) The equation $p_{2n+1}(2a) = 2Y^2$ has no solutions.

b) If $4 \mid 2a$ the equation $p_{4n}(2a) = 2Y^2$ has only the solution $n = 0$.

c) If $2a = 2^t.a'$ where a' is odd and $t \geq 2$ is even, then the equation $p_{4n+2}(2a) = 2Y^2$ has no solutions.

d) If $2a = 2^t.a'$ where $t \geq 3$ is odd and $a' \equiv -1 \pmod 4$ or $a' \equiv 5 \pmod 8$ then the equation $p_{4n+2}(2a) = 2Y^2$ has no solutions.

Proof. a) From (4.15) $p_{2n+1}(2a)$ is odd and therefore $p_{2n+1}(2a) \neq 2Y^2$.

b) From (4.8) and (4.11) clearly

$$p_{4n}(2a) = p_{2n}(2a)\, q_{2n}(2a)$$

where $(p_{2n}(2a), q_{2n}(2a)) = 1$ or 2. Thus if $p_{4n}(2a) = 2Y^2$ we require $q_{2n}(2a) = X_1^2$ or $2X_1^2$ and from theorems 4.1 and 4.2 the only possibility is $n = 0$.

c) From (4.8) and (4.11) and (4.15)

$$p_{4n+2}(2a) = p_{2n+1}(2a)\, q_{2n+1}(2a)$$

where $(p_{2n+1}(2a), q_{2n+1}(2a)) = 1$ and so if $p_{4n+2}(2a) = 2X^2$, since $p_{2n+1}(2a)$ is odd we require $q_{2n+1}(2a) = 2X_1^2$. Since t is even, however, from theorem 4.2 this is impossible.

d) As in c) above we require again $q_{2n+1}(2a) = 2X_1^2$, but under the given conditions, from theorem 4.2 this is again impossible.

These are the only results we have been able to obtain in this case.

CHAPTER 5.

At the beginning of this final chapter we prove various results concerning the solutions, in integers X and Y, of the equations $X^4 - dY^2 = \pm 1, \pm 4$; $X^2 - dY^4 = \pm 1, \pm 4$; $X^2 - dN^2Y^4 = \pm 1, \pm 4$ and $N^2X^4 - dY^2 = \pm 1, \pm 4$ where d and N are given square-free integers. These theorems are deduced from those proved in chapters 1 - 4.

Finally we compare our results with those obtained by Cohn, Ljunggren and Mordell in (2 - 5) and (7 - 13).

We continue to deal with the equations in the four groups of chapters 1 - 4. Throughout, we give only non-negative solutions.

Theorems 5.1, 5.2, 5.9 and 5.10 are due to J.H.E.Cohn and are taken from (2) and (4).

THEOREM 5.1. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = -4$. Then

(a) The equation $X^4 - dY^2 = -4$ has

(i) two solutions, (1,1) and (2,2), if d = 5;

(ii) one solution (6,10), if d = 13;

(iii) one solution, $(a^{\frac{1}{2}},b)$ if a is a perfect square;

(iv) no solutions otherwise.

In particular, the equation $4X^4 - dY^2 = -1$ has

(v) one solution, (1,1), if d = 5;

(vi) one solution, (3,5), if d = 13;

(vii) no solutions otherwise.

(b) The equation $X^4 - dY^2 = 4$ has no solutions.

(c) The equation $X^4 - dY^2 = -1$ has no solutions.

(d) The equation $X^4 - dY^2 = 1$ has

(i) two solutions, (1,0) and (3,4), if d = 5;

(ii) two solutions, (1,0) and (99,1820), if d = 29;

(iii) one solution, (1,0) otherwise.

Proof. (a) From (I.I) the solutions of $X^4 - dY^2 = -4$ are given by $X^2 = Q_{2n-1}(a)$, $Y = bP_{2n-1}(a)$, and from (I.III) those of $4X^4 - dY^2 = -1$ are given by $2X^2 = \frac{1}{2}Q_{6n-3}(a)$, $Y = \frac{1}{2}bP_{6n-3}(a)$. The results now follow from theorem 1.1.

(b) From (I.II) the solutions of $X^4 - dY^2 = 4$ are given by $X^2 = Q_{2n}(a)$, $Y = bP_{2n}(a)$ and the result follows from theorem 1.1.

(c) From (I.III) the solutions of $X^4 - dY^2 = -1$ are given by $X^2 = \frac{1}{2}Q_{6n-3}(a)$, $Y = \frac{1}{2}bP_{6n-3}(a)$ and the result follows from theorem 1.2.

(d) From (I.IV) the solutions of $X^4 - dY^2 = 1$ are given by $X^2 = \frac{1}{2}Q_{6n}(a)$, $Y = \frac{1}{2}bP_{6n}(a)$. The results now follow from theorem 1.2.

This completes the proof.

THEOREM 5.2. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = -4$. Then

(a) The equation $X^2 - dY^4 = -4$ has

(i) one solution, $(a,b^{\frac{1}{2}})$, if b is a perfect square;

(ii) no solutions otherwise.

In particular, the equation $X^2 - 4dY^4 = -1$ has no solutions.

(b) The equation $X^2 - dY^4 = 4$ has

(i) three solutions, (2,0), (3,1) and (322,12), if d = 5;

(ii) two solutions, (2,0) and $(a^2 + 2, a^{\frac{1}{2}}b^{\frac{1}{2}})$ if a and b are both perfect squares;

(iii) one solution, (2,0) otherwise.

In particular, the equation $X^2 - 4dY^4 = 1$ has

(iv) two solutions, (1,0) and (161,6), if d = 5;

(v) one solution, (1,0), otherwise.

(c) The equation $X^2 - dY^4 = -1$ has

(i) one solution, $(\frac{1}{2}(a^3 + 3a), (\frac{1}{2}b(a^2 + 1))^{\frac{1}{2}})$, if $\frac{1}{2}(a^2 + 1)$ and b are both perfect squares;

(ii) no solutions otherwise.

(d) The equation $X^2 - dY^4 = 1$ has

(i) two solutions, (1,0) and (9,2), if d = 5;

(ii) one solution, (1,0), otherwise.

Proof. (a) From (I.I) the solutions of $X^2 - dY^4 = -4$ are given by $X = Q_{2n-1}(a)$, $Y^2 = bP_{2n-1}(a)$. Let $b = b't^2$, where b' = 1 if b is a perfect square and b' is a square-free integer greater than 1 otherwise. We now require $P_{2n-1}(a) = b'Y_1^2$, for some integer Y_1. If a = 1, d = 5 and b = 1 and therefore, from theorem 1.13, if $b' > 1$, there are no solutions.

If b' = 1, from theorem 1.3 there is just one solution, $P_1(a) = 1$.

This proves (a)(i) and (a)(ii).

Since, as in chapter 1, b is clearly odd, that the equation $X^2 - 4dY^4 = -1$ has no solutions follows from the above. However, the result may also be deduced by a simple congruence arguement.

(b) From (I.II) the solutions of $X^2 - dY^4 = 4$ are given by $X = Q_{2n}(a)$, $Y^2 = bP_{2n}(a)$. Let $b = b't^2$ as in (a). Then we require $P_{2n}(a) = b'Y_1^2$ for some integer Y_1.

From theorem 1.13, if $b' > 1$, there is only one solution, $P_0(a) = b'.0^2$. If b' = 1, from theorem 1.3 there are just the

solutions $P_0(a) = 0^2$, $P_2(a) = a$, if a is a perfect square, and $P_{12}(1) = 12^2$.

This proves (b)(i) - (b)(iii).

The solutions of $X^2 - 4dY^4 = 1$ are given by $X = \frac{1}{2}x$, $Y = \frac{1}{2}y$, where $x^2 - dy^4 = 4$. Since, as in chapter 1, a and b are both odd, (b)(iv) and (b)(v) now follow from (b)(i) - (b)(iii).

(c) From (I.III) the solutions of $X^2 - dY^4 = -1$ are given by $X = \frac{1}{2}Q_{6n-3}(a)$, $Y^2 = \frac{1}{2}bP_{6n-3}(a)$. Let $b = b't^2$ as in (a). Then we require $P_{6n-3}(a) = 2b'Y_1^2$ for some integer Y_1.

From theorem 1.14, if $b' > 1$, there are no solutions.

If $b' = 1$, from theorem 1.4 there is just the solution $P_3(a) = a^2 + 1$, if $\frac{1}{2}(a^2 + 1)$ is a perfect square.

This completes the proof of (c).

(d) From (I.IV) the solutions of $X^2 - dY^4 = 1$ are given by $X = \frac{1}{2}Q_{6n}(a)$, $Y^2 = \frac{1}{2}bP_{6n}(a)$. Let $b = b't^2$ as in (a). Then we require $P_{6n}(a) = 2b'Y_1^2$ for some integer Y_1.

If $b' > 1$, from theorem 1.14 the only solution is $P_0(a) = 2b'.0^2$.

If $b' = 1$, from theorem 1.4 there are just the solutions $P_0(a) = 2.0^2$ and $P_6(1) = 2.2^2$.

This completes the proof of the theorem.

THEOREM 5.3. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = -4$. Let N be an odd square-free integer, $N > 1$, such that there exists a solution (X,Y) of the equation $X^2 - dY^2 = -4$ for which $N \mid X$. Let (x,y) be the least positive solution of $X^2 - dY^2 = -4$ with this property. Then

(a) The equation $N^2X^4 - dY^2 = -4$ has

(i) one solution (X_1, y) if $x = NX_1^2$ for some integer X_1;

(ii) no solutions otherwise.

(b) The equation $N^2X^4 - dY^2 = 4$ has no solutions.

(c) The equation $N^2X^4 - dY^2 = -1$ has no solutions.

(d) The equation $N^2X^4 - dY^2 = 1$ has no solutions.

Proof. (a) From (I.I) the solutions of $N^2X^4 - dY^2 = -4$ are given by $NX^2 = Q_{2n-1}(a)$, $Y = bP_{2n-1}(a)$ and the result follows from theorem 1.16.

(b) From (I.II) the solutions of $N^2X^4 - dY^2 = 4$ are given by $NX^2 = Q_{2n}(a)$ $Y = bP_{2n}(a)$. From (I.I), clearly, $N \mid Q_r(a)$ for some odd integer r, and so the result follows from lemma 1.8.

(c) From (I.III) the solutions of $N^2X^4 - dY^2 = -1$ are given by $NX^2 = \frac{1}{2}Q_{6n-3}(a)$, $Y = \frac{1}{2}bP_{6n-3}(a)$ and the result follows from theorem 1.17 since $N \mid Q_r(a)$ for some odd integer r.

(d) From (I.IV) the solutions of $N^2X^4 - dY = 1$ are given by $NX^2 = \frac{1}{2}Q_{6n}(a)$, $Y = \frac{1}{2}bP_{6n}(a)$. Since $N \mid Q_r(a)$ for some odd integer r, the result follows from lemma 1.8.

This completes the proof of the theorem.

THEOREM 5.4. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = -4$. Let N be an odd square-free integer, $N > 1$, such that there exists a solution (X,Y) of the equation $X^2 - dY^2 = 4$ for which $N \mid X$. Let (x,y) be the least positive solution of $X^2 - dY^2 = 4$ with this property. Then

(a) The equation $N^2X^4 - dY^2 = -4$ has no solutions.

(b) The equation $N^2X^4 - dY^2 = 4$ has

(i) one solution (X_1, y) if $x = NX_1^2$ for some integer X_1;

(ii) no solutions otherwise.

(c) The equation $N^2X^4 - dY^2 = -1$ has no solutions.

(d) The equation $N^2X^4 - dY^2 = 1$ has

(i) one solution $(X_1, \frac{y}{2})$ if $x = 2NX_1^2$ for some integer X_1;

(ii) no solutions otherwise.

Proof. (a) From (I.I) the solutions of $N^2X^4 - dY^2 = -4$ are given by $NX^2 = Q_{2n-1}(a)$, $Y = bP_{2n-1}(a)$. From (I.II) we see that $N \mid Q_{2r}(a)$ for some integer r and so the result follows from lemma 1.8.

(b) From (I.II) the solutions of $N^2X^4 - dY^2 = 4$ are given by $NX^2 = Q_{2n}(a)$, $Y = bP_{2n}(a)$ and the result follows from theorem 1.16.

(c) From (I.III) the solutions of $N^2X^4 - dY^2 = -1$ are given by $NX^2 = \frac{1}{2}Q_{6n-3}(a)$, $Y = \frac{1}{2}bP_{6n-3}(a)$ and as in (a) the result follows from lemma 1.8.

(d) From (I.IV) the solutions of $N^2X^4 - dY = 1$ are given by $NX^2 = \frac{1}{2}Q_{6n}(a)$, $Y = \frac{1}{2}bP_{6n}(a)$ and the result follows from theorem 1.17.

This completes the proof of the theorem.

THEOREM 5.5. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = -4$. Let N be an odd square-free integer, $N > 1$, such that there exists a solution (X,Y) of $X^2 - dY^2 = -4$ for which $N \mid Y$. Let $bN = MR^2$ where $M = 1$ or M is a square-free integer, $M > 1$. Then there exists a solution (X,Y) of the equation $X^2 - dY^2 = -4$ for which $bM \mid Y$, and

(a) The equation $X^2 - dN^2Y^4 = -4$ has

(i) one solution (x,y) if (x, Ny^2) is the least positive solution of $X^2 - dY^2 = -4$ for which $bM \mid Y$;

(ii) one solution (a,t) if $b = b't^2$, $N = b'$;

(iii) no solutions otherwise.

(b) The equation $X^2 - dN^2Y^4 = 4$ has

(i) two solutions, (2,0) and $(a^2 + 2, a^{\frac{1}{2}}t)$ if $b = b't^2$, $N = b'$ and a is a perfect square;

(ii) one solution (2,0) otherwise.

(c) The equation $X^2 - dN^2Y^4 = -1$ has

(i) one solution (x,y) if $(2x, 2Ny^2)$ is the least positive solution of $X^2 - dY^2 = -4$ for which $bM|Y$;

(ii) one solution, $(\frac{1}{2}(a^3 + 3a), (\frac{1}{2}(a^2 + 1))^{\frac{1}{2}}t)$, if $b = b't^2$, $N = b'$ and $\frac{1}{2}(a^2 + 1)$ is a perfect square;

(iii) no solutions otherwise.

(d) The equation $X^2 - dN^2Y^4 = 1$ has

(i) two solutions, (1,0) and (649,6), if $d = 13$, $N = 5$;

(ii) one solution, (1,0), otherwise.

Proof. We show first that there exists a solution, (X,Y), of the equation $X^2 - dY^2 = -4$ for which $bM|Y$. For, from (I.I) the solutions of $X^2 - dY^2 = -4$ are given by $X = Q_{2n-1}(a)$, $Y = bP_{2n-1}(a)$. Thus there exists an odd integer r such that $N|P_r(a)$. From lemma 1.1, therefore $N|P_{sr}(a)$ for all integers s. Now $b|a^2 + 4$ and so from (1.27) and lemma 1.1 $b|P_{sb}(a)$ for all integers s. In particular, therefore, $N|P_{rb}(a)$, $b|P_{rb}(a)$. Thus $M|P_{rb}(a)$. But since r and b are both odd, $Q_{rb}(a)^2 - d(bP_{rb}(a))^2 = -4$ which gives the result.

We also note that, since $M|P_{rb}(a)$ where rb is odd, from lemma 1.6 $(M,Q_n(a)) = 1$ for all integers n.

(a) From (I.I) the solutions of $X^2 - dN^2Y^4 = -4$ are given by $X = Q_{2n-1}(a)$, $NY^2 = bP_{2n-1}(a)$. Thus we require $MR^2Y^2 = b^2P_{2n-1}(a)$ or $P_{2n-1}(a) = MY_1^2$, for some integer Y_1.

Since $(M,Q_n(a)) = 1$ for all integers n, if $M > 1$, from theorem 1.18(c) we have just the results given in (a)(i).

If $M = 1$, from theorem 1.3 we have just the solution $P_1(a) = 1^2$, This gives the result stated in (a)(ii).

This completes the proof of (a).

(b) From (I.II) the solutions of $X^2 - dN^2Y^4 = 4$ are given by $X = Q_{2n}(a)$, $NY^2 = bP_{2n}(a)$. Thus we require $MR^2Y^2 = b^2P_{2n}(a)$ or $P_{2n}(a) = MY_1^2$ for some integer Y_1.

Since $(M, Q_n(a)) = 1$ for all integers n, if $M > 1$, from theorem 1.18(c) there is just the solution $P_o(a) = M.0^2$.

If $M = 1$, since $N \neq 1$, $b \neq 1$, and so from theorem 1.3 we have just the solutions $P_o(a) = 0^2$, and $P_2(a) = a$ if a is a perfect square.

This completes the proof of (b).

(c) From (I.III) the solutions of $X^2 - dN^2Y^4 = -1$ are given by $X = \frac{1}{2}Q_{6n-3}(a)$, $NY^2 = \frac{1}{2}bP_{6n-3}(a)$. Thus we require $2MR^2Y^2 = b^2P_{6n-3}(a)$ or $P_{6n-3}(a) = 2MY_1^2$ for some integer Y_1.

Since $(M, Q_n(a)) = 1$ for all integers n, the results follow from theorem 1.18(d) and theorem 1.4.

(d) From (I.IV) the solutions of $X^2 - dN^2Y^4 = 1$ are given by $X = \frac{1}{2}Q_{6n}(a)$, $NY^2 = \frac{1}{2}bP_{6n}(a)$ and so we require $P_{6n}(a) = 2MY_1^2$ for some integer Y_1. The results now follow from theorem 1.18(d) and theorem 1.4.

This completes the proof of the theorem.

THEOREM 5.6. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of the equation $X^2 - dY^2 = -4$. Let N be an odd square-free integer, $N > 1$, such that there exists no solution (X,Y) of $X^2 - dY^2 = -4$ for which $N \mid Y$. Let $bN = MR^2$, where $M = 1$ or M is a square-free integer, $M > 1$. Then there exists solution (X,Y) of

$X^2 - dY^2 = 4$ for which $bM|Y$, and

(a) The equation $X^2 - dN^2Y^4 = -4$ has no solutions.

(b) The equation $X^2 - dN^2Y^4 = 4$ has

(i) two solutions, (2,0) and (x,y) if (x,Ny^2) is the least positive solution of $X^2 - dY^2 = 4$ for which $bM|Y$:

(ii) two solutions, (2,0) and (384 238 404,396) if d = 29, N = 455;

(iii) one solution, (2,0), otherwise.

(c) The equation $X^2 - dN^2Y^4 = -1$ has no solutions.

(d) The equation $X^2 - dN^2Y^4 = 1$ has

(i) two solutions, (1,0) and (x,y) if $(2x,2Ny^2)$ is the least positive solution of $X^2 - dY^2 = 4$ for which $bM|Y$;

(ii) two solutions, (1,0) and (25921,12) if d = 5, N = 161;

(iii) one solution, (1,0) otherwise.

Proof. We show first that there exists a solution (X,Y) of the equation $X^2 - dY^2 = 4$ for which $bM|Y$. For, from (I.II), the solutions of $X^2 - dY^2 = 4$ are given by $X = Q_{2n}(a)$, $Y = bP_{2n}(a)$. Now in chapter 1 we showed that every integer divides $P_r(a)$ for some r and so $N|P_s(a)$ for some s. From (I.I) we see that if s is odd, this contradicts the definition of N. Thus s is even. From lemma 1.1, now $N|P_{sr}(a)$ for every integer r. Also, as in the proof of theorem 5.5, $b|P_{br}(a)$ for all integers r. Thus, in particular, $N|P_{sb}(a)$, $b|P_{sb}(a)$ and so $M\ P_{sb}(a)$. Since s is even, $Q_{sb}(a)^2 - db^2P_{sb}(a)^2 = 4$ which gives the result.

(a) It is easily seen, from the definition of N, that the equation $X^2 - dN^2Y^4 = -4$ has no solutions.

(b) From (I.II) the solutions of $X^2 - dN^2Y^4 = 4$ are given by $X = Q_{2n}(a)$, $NY^2 = bP_{2n}(a)$. Thus we require $P_{2n}(a) = MY_1^2$ for some integer Y_1. Now since $a^2 - db^2 = -4$, $M \neq 1$. Similarly $M \nmid P_r(a)$ for any odd integer r.

The result now follows from theorems 1.18(a) and 1.19(a).

(c) As in (a) it is easily seen that the equation $X^2 - dN^2Y^4 = -1$ has no solutions.

(d) From (I.IV) the solutions of $X^2 - dN^2Y^4 = 1$ are given by $X = \frac{1}{2}Q_{6n}(a)$, $NY^2 = \frac{1}{2}bP_{6n}(a)$. Thus again we require $P_{6n}(a) = 2MY_1^2$, for some integer Y_1. As in (b), $M \neq 1$, and $M \nmid P_r(a)$ for any odd integer r and the results follow from theorems 1.18(b) and 1.19(b).

This completes the proof of the theorem.

THEOREM 5.7. Let d be an even square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions. Let (2a,2b) be the fundamental solution of $X^2 - dY^2 = -4$. Then

(a) The equation $X^4 - dY^2 = -4$ has no solutions.

(b) The equation $X^4 - dY^2 = 4$ has no solutions.

(c) The equation $X^4 - dY^2 = 1$ has

(i) one solution (1,0).

Proof. Since d is even, the equations $X^4 - dY^2 = \pm 4$ are both impossible modulo 8. This proves (a) and (b).

(c) Since d is even, a is odd. From (II.IV) the solutions of $X^4 - dY^2 = 1$ are given by $X^2 = \frac{1}{2}Q_{2n}(2a)$, $Y = bP_{2n}(2a)$ where a is odd.

The result now follows from theorem 2.1.

This completes the proof.

THEOREM 5.8. Let d be an even square-free integer such that equation $X^2 - dY^2 = -4$ has solutions. Let (2a,2b) be the fundamental solution of $X^2 - dY^2 = -4$. Let N be an odd square-free integer, $N > 1$, such that there exists a solution, (X,Y), of the equation $X^2 - dY^2 = -4$ for which $N \mid Y$. Then

(a) The equation $X^2 - dY^4 = -4$ has no solutions.

(b) The equation $X^2 - dN^2Y^4 = -4$ has no solutions.

(c) The equation $X^2 - dY^4 = 1$ has

(i) one solution, (1,0).

(d) The equation $X^2 - dN^2Y^4 = 1$ has

(i) one solution, (1,0).

Proof. Since d is even and N is odd the equations $X^2 - dY^4 = -4$ and $X^2 - dN^2Y^4 = -4$ are both impossible modulo 16. This proves (a) and (b).

(c) Since d is even, a and b are odd. From (II.IV) the solutions of $X^2 - dY^4 = 1$ are given by $X = \frac{1}{2}Q_{2n}(2a)$ $Y^2 = bP_{2n}(2a)$. From (2.8), therefore, we require

$$bP_n(2a)\, Q_n(2a) = Y^2.$$

Now since $Q_n(a)^2 - db^2P_n(2a)^2 = 4$, $(b, Q_n(2a)) = 1$. Thus, if we write $b = b't^2$ where $b' = 1$ or b' is a square-free integer $b' > 1$, by virtue of (2.11) we require either

$$P_n(2a) = b'Y_1^2, \quad Q_n(2a) = Y_2^2$$

which is impossible from (2.14), or

$$P_n(2a) = 2b'Y_1^2, \quad Q_n(2a) = 2Y_2^2$$

where, from the first equation and (2.15) we require n even. But then the second equation has only the solution $n = 0$ from theorem 2.1.

This completes the proof of (c).

(d) From (II.IV) the solutions of $X^2 - dN^2Y^4 = 1$ are given by $X = \frac{1}{2}Q_{2n}(2a)$, $NY^2 = bP_{2n}(2a)$. From (2.8) therefore we require

$$bP_n(2a)\, Q_n(2a) = NY^2.$$

If $(N, Q_n(2a)) = 1$, as in (c) we require either

$$Q_n(2a) = Y_1^2$$

which is impossible from (2.14), or

$$Q_n(2a) = 2Y_1^2$$

where n is even, which from theorem 2.1 implies n = 0.

If $(N, Q_n(2a)) > 1$, from (II.I) by virtue of the definition of N we see that there exists an odd integer r such that $(Q_n(2a), P_r(2a))$ has an odd factor greater than 1. However, as was observed in chapter 2, the proof of lemma 1.6 did not depend upon the fact that a was odd. Therefore the result carries over to this case and, since r is odd, $(Q_n(2a), P_r(2a)) \mid 4$. Thus $(Q_n(2a), N) \not> 1$, and the result is proved.

This completes the proof of the theorem.

THEOREM 5.9. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions but the equation $X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = 4$. Then

(a) The equation $X^4 - dY^2 = 4$ has

(i) one solution, $(a^{\frac{1}{2}}, b)$ if a is a perfect square;

(ii) no solutions otherwise.

(b) The equation $X^4 - dY^2 = 1$ has

(i) one solution (1,0).

Proof. (a) From (III.I) the solutions of $X^4 - dY^2 = 4$ are given by $X^2 = q_n(a)$, $Y = bp_n(a)$ and the result follows from theorem 3.1.

(b) From (III.II) the solutions of $X^4 - dY^2 = 1$ are given by $X^2 = \frac{1}{2}q_{3n}(a)$, $Y = \frac{1}{2}bp_{3n}(a)$ and the result follows from theorem 3.2.

This completes the proof.

THEOREM 5.10. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions but the equation $X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = 4$. Then

(a) The equation $X^2 - dY^4 = 4$ has

(i) two solutions, (2,0) and $(a,b^{\frac{1}{2}})$, if b is a perfect square and a is not a perfect square;

(ii) three solutions, (2,0), $(a,b^{\frac{1}{2}})$ and $(a^2 - 2, a^{\frac{1}{2}}b^{\frac{1}{2}})$ if a and b are both perfect squares;

(iii) two solutions, (2,0) and $\left(a^3 - 3a, \left(b(a^2 - 1)\right)^{\frac{1}{2}}\right)$ if $a^2 - 1$ and b are both three times perfect squares;

(iv) one solution, (2,0), otherwise.

(b) The equation $X^2 - dY^4 = 1$ has

(i) two solutions, (1,0) and $\left(\frac{1}{2}(a^3 - 3a), \left(\frac{1}{2}b(a^2 - 1)\right)^{\frac{1}{2}}\right)$ if $\frac{1}{2}(a^2 - 1)$ and b are both perfect squares;

(ii) one solution, (1,0), otherwise.

Proof. (a) From (III.I) the solutions of $X^2 - dY^4 = 4$ are given by $X = q_n(a)$, $Y^2 = bp_n(a)$. Let $b = b't^2$ as in theorem 5.2. We now require $p_n(a) = b'Y_1^2$ for some integer Y_1.

If $b' = 1$, from theorem 3.3 there are just the solutions $p_0(a) = 0^2$, $p_1(a) = 1$ and $p_2(a) = a$ if a is a perfect square.

If $b' > 1$, from theorem 3.13 there are just the solutions $p_0(a) = b'.0^2$ and $p_3(a) = a^2 - 1$ if $b' = 3$ and $a^2 - 1 = 3Y_2^2$ for some integer Y_2.

(b) From (III.II) the solutions of $X^2 - dY^4 = 1$ are given by $X = \frac{1}{2}q_{3n}(a)$, $Y^2 = \frac{1}{2}bp_{3n}(a)$. Put $b = b't^2$ as before. Then we require $p_{3n}(a) = 2b'Y_1^2$ for some integer Y_1.

If $b' = 1$, from theorem 3.4 there are just the solutions $p_0(a) = 2.0^2$ and $p_3(a) = a^2 - 1$ if $\frac{1}{2}(a^2 - 1)$ is a perfect square.

If $b' > 1$, from theorem 3.13 there are just the solutions $p_0(a) = b'.0^2$ and $p_3(a) = a^2 - 1$ if $b' = 3$ and $a^2 - 1 = 6Y_2^2$ for some integer Y_2. But since $a^2 - 4 = db^2$, this last possibility requires

$$6Y_2^2 - 3 = 9dt^2$$

which is impossible modulo 9.

This completes the proof of the theorem.

THEOREM 5.11. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions, but the equation $X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = 4$. Let N be an odd square-free integer such that there exists a solution (X,Y) of the equation $X^2 - dY^2 = 4$ for which $N|X$. Let (x,y) be the least positive solution of $X^2 - dY^2 = 4$ with this property. Then

(a) The equation $N^2X^4 - dY^2 = 4$ has

(i) one solution (X_1, y) if $x = NX_1^2$ for some integer X_1;

(ii) no solutions otherwise.

(b) The equation $N^2X^4 - dY^2 = 1$ has

(i) one solution $(X_1, y/2)$ if $x = 2NX_1^2$ for some integer X_1;

(ii) no solutions otherwise.

Proof. (a) From (III.I) the solutions of $N^2X^4 - dY^2 = 4$ are given by $NX^2 = q_n(a)$, $Y = bp_n(a)$ and the results follow from theorem 3.16.

(b) From (III.II) the solutions of $N^2X^4 - dY = 1$ are given by $NX^2 = \frac{1}{2}q_{3n}(a)$, $Y = \frac{1}{2}bp_{3n}(a)$ and the results follow from theorem 3.17.

This completes the proof.

THEOREM 5.12. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions, but the equation

$X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd. Let (a,b) be the fundamental solution of $X^2 - dY^2 = 4$. Let N be an odd square-free integer, $N > 1$. Let $bN = MR^2$ where $M = 1$ or M is a square-free integer, $M > 1$. Then there exists a solution of $X^2 - dY^2 = 4$ for which $bM \mid Y$ and

(a) The equation $X^2 - dN^2Y^4 = 4$ has

(i) two solutions $(2,0)$ and (a,t), if $b = b't^2$, $N = b'$ and a is not a perfect square;

(ii) three solutions, $(2,0)$, (a,t) and $(a^2 - 2, ta^{\frac{1}{2}})$ if $b = b't^2$, $N = b'$ and a is a perfect square;

(iii) two solutions, $(2,0)$ and (x,y) if (x,Ny^2) is the least positive solution of $X^2 - dY^2 = 4$ for which $bM \mid Y$;

(iv) one solution, $(2,0)$, otherwise.

(b) The equation $X^2 - dN^2Y^4 = 1$ has

(i) two solutions, $(1,0)$ and $(\frac{1}{2}(a^3 - 3a), \left(t(\frac{1}{2}(a^2 - 1)\right)^{\frac{1}{2}})$ if $b = b't^2$ $N = b'$ and $\frac{1}{2}(a^2 - 1)$ is a perfect square;

(ii) two solutions, $(1,0)$ and (x,y) if $(2x, 2Ny^2)$ is the least positive solution of $X^2 - dY^2 = 4$ for which $bM \mid Y$;

(iii) one solution, $(1,0)$, otherwise.

Proof. From (III.I) the solutions of $X^2 - dY^2 = 4$ are given by $X = q_n(a)$, $Y = bp_n(a)$ and from chapter 3 we see that $M \mid p_s(a)$ for some integer s. Thus $bM \mid Y$ for some solution (X,Y) of $X^2 - dY^2 = 4$.

(a) From (III.I) the solutions of $X^2 - dN^2Y^4 = 4$ are given by $X = q_n(a)$, $NY^2 = bp_n(a)$. Thus we require $p_n(a) = MY_1^2$ for some integer Y_1. If $M = 1$, from theorem 3.3 there are just the solutions $p_0(a) = 0^2$, $p_1(a) = 1^2$ and $p_2(a) = a$ if a is a perfect square.

If $M > 1$, from theorem 3.18(a) and (c) and theorem 3.19 (a)

there are just the solutions $p_o(a) = M.0^2$ and $p_\rho(a) = MY_1^2$, where ρ is the rank of apparition of M with respect to the sequence $p_n(a)$.

This concludes the proof of (a).

(b) From (III.II) the solutions of $X^2 - dN^2Y^4 = 1$ are given by $X = \frac{1}{2}q_{3n}(a)$, $NY^2 = \frac{1}{2}bp_{3n}(a)$. Thus we require $p_{3n}(a) = 2MY_1^2$ for some integer Y_1 and the results follow from theorem 3.4, theorem 3.18(b) and (d) and theorem 3.19 (b).

This completes the proof of the theorem.

THEOREM 5.13. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions and the equation $X^2 - dY^2 = 4$ has only solutions (X,Y) for which X and Y are both even. Let (2a, 2b) be the fundamental solution of $X^2 - dY^2 = 4$. Suppose that $db^2 \not\equiv 3$ or 63 (mod 64). Then the equation $X^4 - dY^2 = 4$ has no solutions.

Proof. From (IV.I) the solutions of $X^4 - .dY^2 = 4$ are given by $X^2 = q_n(2a)$, $Y = 2bp_n(2a)$. Since all solutions of $X^2 - dY^2 = 4$ are even we require X to be even, i.e. $4 \mid q_n(2a)$. From (4.14), therefore, n is odd. Thus from theorem 4.1 $q_n(2a) \neq X^2$ except possibly if $2a = 2^{2s}a'$ where $s \geq 1$ and $a' \equiv 1 \pmod 8$.

But $4a^2 - 4 = 4db^2$, i.e. $2^{4s-2}a'^2 - 1 = db^2$. Therefore,

if $s = 1$, $db^2 \equiv 3 \pmod{64}$.

if $s>1$, $db^2 \equiv -1 \pmod{64}$.

But this implies $db^2 \equiv 3$ or 63 (mod 64), contrary to our supposition.

This completes the proof of the theorem.

Now it should be observed that Cohn, in (2), proved the results stated in theorems 5.1 and 5.2 for any non-square integer D with the property that the equation $X^2 - DY^2 = -4$ has solutions (X,Y) for which X and Y are both odd, whereas theorems 5.1 and 5.2 are stated only for square-free values of D.

Clearly this difference is irrelevant in the case of theorem 5.1 but not in the case of theorem 5.2. For example (2) covers the values D = 845 and 125 which theorem 5.2 does not.

However, if we are seeking solutions (X,Y) of the equations

$$X^2 - DY^4 = \pm 1, \pm 4$$

where $D = dN^2$ and d is square-free, this is equivalent to seeking solutions of

$$X^2 - dN^2Y^4 = \pm 1, \pm 4.$$

Also, if the equation $X^2 - DY^2 = -4$ has solutions (X,Y) for which X and Y are both odd then clearly the equation $X^2 - dN^2Y^2 = -4$ has solutions with the same property. This in turn implies that the equation

$$X^2 - dY^2 = -4$$

has solutions (X,Y) for which X and Y are both odd.

The solutions of $X^2 - DY^2 = -4$ are to be found among those of $X^2 - dY^2 = -4$ and the least positive solution (X,Y) of $X^2 - dY^2 = -4$ for which $N|Y$ is clearly the fundamental solution of $X^2 - DY^2 = -4$. Thus the results for D corresponding to those stated in theorem 5.2 (a) for d are in fact equivalent to those stated in theorem 5.5 (a) for d and N.

There is obviously a similar connection between the results of theorem 5.2(b) stated for general non-square D and theorem 5.5 (b). In fact, here our result is a slight improvement on that of Cohn in (2). For Cohn showed that, with the one exception D = 5, the equation $X^2 - DY^4 = 4$ has only the trivial solution (2,0) and one other if the fundamental

solution of $X^2 - DY^2 = -4$ is of the form $A^2 + B^2D^{\frac{1}{2}}$. Theorems 5.2 (b) and 5.5 (b) show that the fundamental solution cannot be of this form unless $D = dN^2$ where d is square-free and $A^2 + NB^2d^{\frac{1}{2}}$ is the fundamental solution of $X^2 - dY^2 = -4$. Thus, for example, we have shown immediately that the equation $X^2 - 125Y^4 = 4$ has only the trivial solution, since if $d = 5$, the fundamental solution of $X^2 - dY^2 = -4$ is $1 + 1.d^{\frac{1}{2}}$.

In the case of the equation $X^2 - DY^4 = -1$ it would appear at first that we had lost something in presenting the results in this form. For, although, when we consider D with non-trivial square factors, theorem 5.5 (c) (ii) again provides a sharpening of the result in (2) we have the added possibility stated in theorem 5.5 (c) (i).

However, this says that the equation

$$X^2 - DY^4 = -1$$

has a solution if $(2x, 2Ny^2)$ is the least positive solution of $X^2 - dY^2 = -4$ for which $N|Y$. This implies that $(2x, 2y^2)$ is the fundamental solution of $X^2 - DY^2 = -4$. Thus from (6) clearly all the solutions (X,Y) of $X^2 - DY^2 = -4$ are such that X and Y are both even and these values of D are not considered in (2).

Thus in the case where the equation $X^2 - DY^2 = -4$ has odd solutions we have again proved Cohn's results. We have also solved the equation $X^2 - DY^4 = -1$ in some cases not covered by (2), for example $D = 1445$.

Finally, comparing the results of theorem 5.2 (d) stated for general non-square values of D with those of theorem 5.5 (d), we see again that we have proved the results of (2) and also solved the equation $X^2 - DY^4 = 1$ for some

values of D not considered in (2). For example we have shown that the equation $X^2 - 325Y^4 = 1$ has only the solutions (1,0) and (629,6) and that the equation $X^2 - 4901Y^4 = 1$ has only the solution (1,0).

Turning now to theorem 5.6 we see that here we are concerned with non-square D of the form $D = dN^2$ where the equation $X^2 - dY^2 = -4$ has solutions, but the equation $X^2 - DY^2 = -4$ does not. Thus these results are to be compared with those of Cohn in (4), where he proved the results stated in theorem 5.10 for general non-square D with the property that the equation $X^2 - DY^2 = 4$ has solutions (X,Y) for which X and Y are both odd.

Comparing these results we see that theorem 5.6 (b)(i) is equivalent to theorem 5.10 (a)(i) and that if the equation $X^2 - dY^2 = -4$ has solutions, the possibilities stated in theorem 5.10 (a)(ii) and (iii) are excluded.

A similar comparison may be made between (4) and theorems 5.6 (d), 5.10 and 5.12. This shows that we have dealt with all the values of D considered in (4) and some other values not considered there, for example D = 208 and D = 405.

Any even values of D which are dealt with by theorems 5.2, 5.5, 5.6, 5.10 and 5.12 will clearly be of the form $D = 2^{2r}D'$ where D' is odd. Thus theorem 8 deals with yet more values of D, for example D = 2,26 and 50, but of course solves only the equations $X^2 - DY^4 = 1, -4$.

Theorems 5.1 and 5.9 give exactly Cohn's results on the equations $X^4 - DY^2 = \pm 1, \pm 4$ from (2) and (4). Theorems 5.7 and 5.13 deal with some of these equations for values of D not considered in (2) and (4), (for example we prove that the equation $X^4 - 2Y^2 = 1$ has only the solution (1,0)), but these results do not cover many interesting cases.

All the equations considered above have been considered

by Ljunggren in (7 - 11), and he has given upper bounds for the number of solutions and methods of obtaining solutions where they exist in each case. He has also dealt with many of the equations for values of D not considered above, showing in (9), for example, that the equation $X^4 - 143Y^2 = 1$ has only the trivial solution (1,0).

For those values of D which we have considered, however, we have in some cases provided more exact information about the solutions of the equations $X^4 - DY^2 = \pm 1, \pm 4$ and $X^2 - DY^4 = \pm 1, \pm 4$ or given easier methods of determining solutions where they exist.

For example, in (9) Ljunggren has shown that the equation $X^4 - DY^2 = 1$ has, for any non-square value of D, at most two solutions other than the trivial one, (1,0), and given a fairly complicated method for finding solutions. From theorems 5.1, 5.7 and 5.9 we see that in the cases which we have considered we have shown that the equation can have only the trivial equation unless $D = 5$ or $D = 29$.

Similarly, in (7), Ljunggren shows that for any non-square D the equation $X^2 - DY^4 = 1$ has at most two non-trivial solutions. In the cases we have considered we have brought the bound on the possible number of solutions down from two to one.

Ljunggren has also solved the equation $X^2 - DY^4 = -1$ for more values of D than are covered by our results, proving, for example, that the equation $X^2 - 2Y^4 = -1$ has only the solutions (1,1) and (239,13). However his method for finding solutions in a given case is very complicated and ours, as is seen from theorems 5.2, 5.5, and 5.6, is comparatively simple - although again it must be stressed that the initial task of finding the fundamental solutions in any given case may be very tedious.

When we come to consider the equations $N^2X^4 - DY^2 = \pm 1, \pm 4$ again we find that our results are covered to some extent by the work of Ljunggren in (8) and (11). Ljunggren has solved the equations $AX^4 - BY^2 = -1, -4$ for all A and B showing, in (8), that these equations can have at most two solutions in integers positive X and Y. He has also shown, in (11), that if the equation $AX^2 - BY^2 = 4$ has solutions (X,Y) for which X and Y are both odd, then the equations $AX^4 - BY^2 = 1, 4$ have at most two solutions in positive integers. In each case he gives a method for finding solutions where they exist.
It will be readily seen that our equations are special cases of the equations $AX^4 - BY^2 = \pm 1, \pm 4$ but again from theorems 5.3, 5.4 and 5.11 we see that in this special case we have shown that there is at most one solution in positive integers.

One aspect of the problem not dealt with in Ljunggren's work is that of the simultaneous solution of the equations

$$X^2 - dN^2Y^4 = \pm 1, \pm 4$$
$$N^2X^4 - dY^2 = \pm 1, \pm 4.$$

Our results however give the following two theorems.

THEOREM 5.14. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has solutions (X,Y) for which X and Y are both odd. Let N be an odd square-free integer, $N > 1$. Then if one of the equations

$$N^2X^4 - dY^2 = \pm 1, \pm 4$$
$$X^2 - dN^2Y^4 = \pm 1, \pm 4$$

has solutions, there are no solutions of the other seven equations, except in the cases listed below. We have an effective method for actually solving the equations in a given example.

(i) $18^2 - 13.5^2.1^4 = -1$
$649^2 - 13.5^2.6^4 = 1.$ } $d = 13,\ N = 5.$

(ii) $N^2K^4 - d = -4$
$(N^2K^4 + 2)^2 - dN^2K^4 = 4.$ } $d = N^2K^4 + 4$

(iii) $161.^2 1^4 - 5.144^2 = 1$
$51841^2 - 5.161^2.12^4 = 1.$ } $d = 5,\ N = 161.$

(iv) $N^2K^4 - d.(R^4 = 4$
$(R^8 + 4R^4 + 2)^2 - dN^2(RK)^4 = 4.$ } $d = R^4 + 4,\ NK^2 = d - 2.$

(v) $N^2K^4 - d.(2R)^2 = -4$
$(\frac{1}{2}N^2K^4 + 1)^2 - dN^2(RK)^4 = 1.$ } $d = 2R^2 + 3,\ NK^2 = a^3 + 3a,$ $a^2 + 1 = 2R^2.$

(vi) $9801^2 - 29.455^2.2^4 = 1$
$38423784 02^2 - 29.455^2.396^4 - 4$ } $d = 29,\ N = 455.$

Proof. From (I.I) - (I.IV), it is easily seen that if more than one of the equations

$$N^2X^4 - dY^2 = \pm 1, \pm 4$$
$$X^2 - dN^2Y^4 = \pm 1, \pm 4$$

has solutions, then one of the following six equations must have a solution.

$$Q_m(a)\, Q_n(a) = Y^2 \text{ or } 2Y^2 \quad m \neq n;$$
$$P_m(a)\, P_n(a) = Y^2 \text{ or } 2Y^2 \quad m \neq n$$
$$bP_m(a)\, Q_n(a) = Y^2 \text{ or } 2Y^2$$

From corollary 1.2 the first four are all impossible except that
$P_m(a)P_n(a) = Y^2$
has the solution $m=6$, $n=3$, $a=3$ which gives (i), and
$P_m(a)P_n(a) = 2Y^2$
has the solution $m=12$, $n=6$, $a=5$ which gives (vi).
If $b = 1$, from corollary 1.2 again the last two equations give (ii) - (v) only.

If $b > 1$, from (1.11) clearly $(b, Q_n(a)) = 1$ and so, by virtue of lemma 1.6 we require either

$$P_m(a) = bY_1^2 \text{ or } 2bY_1^2$$

which from theorems 1.13 and 1.14 is impossible, or

$$Q_n(a) = 2Q_{(m,n)}(a)\, Y_2^2$$

which from theorem 1.6 is impossible, or

$$Q_n(a) = Q_{(m,n)}(a)\, Y_2^2$$

which from theorem 1.5 implies that $(m,n) = n$, i.e. $n|m$. From lemma 1.6 we see now that we require

$$P_m(a) = bQ_n(a)Y_1^2 \text{ or } 2bQ_n(a)\, Y_1^2$$

where $m = 2tn$ for some integer t. Thus, from (1.8)

$$P_{tn}(a)\, Q_{tn}(a) = bQ_n(a)\, Y_1^2 \text{ or } 2bQ_n(a)\, Y_1^2$$

If t is odd, from lemma 1.2 $Q_n(a) | Q_{tn}(a)$ and we require

$$P_{tn}(a) = bY_3^2 \text{ or } 2bY_3^2$$

which is again impossible from theorems 1.13 and 1.14. If t is even we see, from (1.8) and lemma 1.1, that $Q_n(a) | P_{tn}(a)$ and so since $(b, Q_n(a)) = 1$, we require

$$Q_{tn}(a) = Y_4^2 \text{ or } 2Y_4^2$$

but none of the possibilities given by theorems 1.1 and 1.2 yields a result.

THEOREM 5.15. Let d be a square-free integer such that the equation $X^2 - dY^2 = -4$ has no solutions, but the equation

$X^2 - dY^2 = 4$ has solutions (X,Y) for which X and Y are both odd. Let N be an odd square-free integer, $N > 1$. Then if one of the equations

$$N^2X^4 - dY^2 = 1,4$$
$$X^2 - dN^2Y^4 = 1,4$$

has solutions, there are no solutions of the other three equations except in the cases

(i) $\left.\begin{aligned} &N^2K^4 - d = 4 \\ &(N^2K^4 - 2)^2 - dN^2K^4 = 4 \end{aligned}\right\}$ $d = N^2K^4 - 4.$

(ii) $\left.\begin{aligned} &N^2K^4 - dR^4 = 4 \\ &(R^8 - 4R^4 + 2)^2 - d.N^2(RK)^4 = 4 \end{aligned}\right\}$ $d = R^4 - 4,\ NK^2 = d + 2.$

(iii) $\left.\begin{aligned} &N^2K^4 - d\,(2R)^2 = 4 \\ &(\tfrac{1}{2}N^2K^4 + 1)^2 - dN^2(RK)^4 = 1 \end{aligned}\right\}$ $d = 2R^2 - 3, NK^2 = a^3 - 3a,$ $a^2 - 1 = 2R^2$

(iv) $\left.\begin{aligned} &N^2K^4 - d.\,(9R)^2 = 1 \\ &(2N^2K^4 - 1)^2 - d.N^2(3RK)^4 = 1 \end{aligned}\right\}$ $9d = 12R^2 - 3,\ a^3 - 3a = 2NK,\ a^2 - 1 = 12R^2$

We have an effective method for actually solving the equations in a given example.

Proof. From (III.I) and (III.II) it is easily seen that if more than one of the equations

$$N^2X^4 - dY^2 = 1, 4$$
$$X^2 - dN^2Y^4 = 1, 4$$

has solutions, then one of the following six equations must have a solution;

$$q_m(a)\ q_n(a) = Y^2 \text{ or } 2Y^2 \quad m \neq n;$$
$$p_m(a)\ p_n(a) = Y^2 \text{ or } 2Y^2 \quad m \neq n;$$
$$bp_m(a)\ q_n(a) = Y^2 \text{ or } 2Y^2.$$

From corollary 3.2 the first four are all impossible. If $b = 1$, corollary 3.1 shows that there are only the solutions (i) - (iii). If $b > 1$, from (3.12) clearly $(b, q_n(a)) = 1$ and from theorems 3.13, 3.14, 3.1 and 3.2 it is easy to deduce that the only other solution is that stated in (iv).
This completes the proof of the theorem.

Now in (13) Mordell gave some explicit formulae for D for which the equation $X^2 - DY^4 = 1$ has only the trivial solution, (1,0). This work covers values of D not covered by our results, for example 37,101 and 197, although we have dealt with many cases not considered by Mordell. Apart from appealing at one point to Ljunggren's result from (10) concerning the solutions of the equation $X^2 - 2Y^4 = -1$, the methods used are elementary and self-contained.

In (5) Cohn, using methods very similar to those of (2), gives other formulae for D for which neither of the equations $X^2 - DY^4 = 1$ and $X^2 - 4DY^4 = 1$ have non-trivial solutions. This work covers values of D not dealt with in (13), for example, $D = 185$, 170 and 365.

As a special case of his results in (13) Mordell proved that the equation $X^2 - DY^4 = 1$ can have only the trivial solution if D is a prime, $D \equiv 5,9$ or 13 (mod 16), $D \neq 5$. He stated at the end of the paper that he had been informed by Professor Ljunggren that Ljunggren had already proved this result although he had not published it.

In (12) Ljunggren published the result for the case $D \equiv 1$ (mod 16) not covered by Mordell's work. In this paper he also proved that the equation $X^4 - DY^2 = 1$ where D is a prime can have only the trivial solution, except in the cases $D = 5$ and $D = 29$ when there are just the solutions (3,4) and (99,1820)

respectively.

We conclude this thesis by giving another condition under which the equation $X^4 - DY^2 = 1$ can have only the trivial solution and proving a similar result for the equation $X^4 - DY^2 = 4$.

THEOREM 5.16. Let d be a square free integer such that the equation $X^2 - dY^2 = -1$ has solutions in integers X and Y. Then

(a) The equation $X^4 - dY^2 = 4$ has no solutions.

(b) If d is even the equation $X^4 - dY^2 = 1$ has only the solution (1,0).

Proof.(a) Since the equation $X^2 - dY^2 = -1$ has solutions, $d \equiv 1,2$ or 5 (mod 8).

If $d \equiv 2 \pmod 8$ from theorem 5.7 the equation $X^4 - dY^2 = 4$ has no solutions.

If $d \equiv 5 \pmod 8$ and the equation $X^2 - dY^2 = -4$ has odd solutions, from theorem 5.1 the equation $X^4 - dY^2 = 4$ has no solutions.

If $d \equiv 1$ or $5 \pmod 8$ and the equation $X^2 - dY^2 = -4$ has only even solutions, then we see that if $x^4 - dy^2 = 4$, x and y are both even, and $4(\frac{1}{2}x)^4 - d(\frac{1}{2}y)^2 = 1$ which is impossible since $d \equiv 1$ or $5 \pmod 8$.

(b) The proof of (b) follows from theorem 5.7.

It will be readily seen that theorem 5.16 (b) covers such values as d = 2,82 and 170 not covered by (12).

REFERENCES.

1. BUMBY, R.T. The Diophantine Equation $3x^4 - 2y^2 = 1$. (Math.Scand. 21 (1967) 144 - 148).

2. COHN, J.H.E. Eight Diophantine Equations. (Proc.London Math.Soc. (3) 16 (1966) 153-166)

3. COHN, J.H.E. Eight Diophantine Equations. Addendum. (Proc.London Math.Soc. (3) 17 (1967) 381.)

4. COHN, J.H.E. Five Diophantine Equations. (Math.Scand. 21 (1967) 61 - 70.)

5. COHN, J.H.E. The Diophantine Equation $y^2 = Dx^4 + 1$. (J.London Math.Soc. 42 (1967) 475 - 476.)

6. LeVEQUE, W.J. Topics in Number Theory. Vol.1. (Reading, Massachusetts. 1956. 145 - 146.)

7. LJUNGGREN, W. Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkorper. Mit Anwendung auf die Losung einer Klasse unbestimmter Gleichungen vierten Grades. (Skr.Norske Vid.Akad.Oslo, Mat.-Naturv. Klasse, 1936, No.12, 73pp.)

8. LJUNGGREN, W Uber die unbestimmte Gleichung $Ax^2 - By^4 = C$. (Arch.for Math.og Naturv.(Oslo) 41 Nr.10 (1938), 18pp).

9. LJUNGGREN, W. Uber die Gleichung $x^4 - Dy^2 = 1$. (Arch.for Math.og Naturv.(Oslo) 45 (1942) 61 - 70.)

10. LJUNGGREN, W. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. (Avh.Norske Vid.Akad.Oslo 1 (1942) Nr.5 27pp.)

11. LJUNGGREN, W. On the Diophantine Equation $Ax^4 - By^2 = C$ ($C = 1,4$).
(Math.Scand. 21 (1967) 149 - 158.)

12. LJUNGGREN, W. Some Remarks on the Diophantine Equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$.
(J.London Math.Soc. 41 (1966) 542 - 544).

13. MORDELL, L.J. The Diophantine Equation $y^2 = Dx^4 + 1$.
(J.London Math.Soc. 39 (1964) 161 - 164.)

14. MORDELL, L.J. Diophantine Equations.
(London. 1969 53- 54.)

15. NAGELL, T. Introduction to Number Theory.
(New York. 1951. 204.)