FIVE DIOPHANTINE EQUATIONS

J. H. E. COHN

1. Introduction.

In a previous paper [2] we discussed the first four equations of Section 4 below (the fifth had no solutions) in the case in which the equation $X^2-dY^2=-4$ had solutions for at least one of which X and Y were both odd. This paper deals with the same problems for those values of d for which

$$X^2 - dY^2 = -4$$

has no such solutions, but for which

$$X^2 - dY^2 = 4$$

has at least one pair of solutions X, Y both of which are odd. It follows immediately that only values of d for which $d \equiv 5 \pmod{8}$ can be covered by this discussion. However, there are values of d which satisfy this condition and are covered neither by [2] nor by this paper, for example d=37. However, our discussion does yield results for many new values of d.

2. Preliminaries.

We first show that in the case we consider here. $X^2-dY^2=-4$ has no solutions at all. For, since $d \equiv 5 \pmod 8$, if there are any solutions X and Y must be either both even or both odd; since we suppose that there are no solutions for which X and Y are both odd, it follows that for any solution $X=2x_1$ and $Y=2y_1$. Then $x_1^2-dy_1^2=-1$. Thus one of x_1,y_1 is even and one odd. Now let $X=x_2$ and $Y=y_2$ be both odd and satisfy

$$x_2^2 - dy_2^2 = 4$$

and let

$$\xi = x_1 x_2 + d y_1 y_2, \qquad \eta = x_1 y_2 + x_2 y_1.$$

Then both ξ and η are odd and

Received September 23, 1966.

$$\xi^2 - d\eta^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = -4$$

which contradicts the assumption that $X^2 - dY^2 = -4$ has no solutions for which X and Y are both odd. Thus we have

(1)
$$X^2 - dY^2 = -4$$
 has no solutions

and in particular

(2)
$$X^2 - dY^2 = -1$$
 has no solutions.

Now suppose that X=a, Y=b is the fundamental solution of $X^2-dY^2=4$. Then the general solution is given by

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

Now if a and b were both even, it would follow that for any solution X and Y would both be even, which contradicts the assumption that there is at least one pair of solution for which both X and Y are odd. Thus at least one of a and b is odd, and so since $d \equiv 5 \pmod{8}$, it follows that they are both odd. We shall retain the symbols a, b to denote this fundamental solution throughout the paper, and define

$$\alpha = \frac{1}{2}(a+bd^{\frac{1}{2}}); \quad \beta = \frac{1}{2}(a-bd^{\frac{1}{2}}).$$

Then

(3)
$$\alpha + \beta = a, \quad \alpha\beta = 1.$$

We now define for all integers n

$$(4) u_n = d^{-\frac{1}{2}}(\alpha^n - \beta^n), v_n = \alpha^n + \beta^n.$$

Then by (3) we have

$$(5) u_{n+2} = a u_{n+1} - u_n$$

$$(6) v_{n+2} = av_{n+1} - v_n$$

$$(7) u_{-n} = -u_n$$

$$(8) v_{-n} = v_n.$$

Also $u_0 = 0$, $u_1 = b$, $v_0 = 2$, $v_1 = a$ and so for all integers n, the numbers u_n and v_n are integers; moreover they are positive for positive n, since $\alpha > \beta > 0$. We also observe that since $X^2 - dY^2 = -4$ has solutions for d = 5 and d = 13, $d \ge 21$, and so since $a^2 = db^2 + 4$,

$$a \geq 5.$$

Calculation gives the following values

We also obtain, using (3)-(8)

$$2u_{m+n} = u_m v_n + u_n v_m$$

$$2v_{m+n} = du_m u_n + v_m v_n$$

$$4 = v_n^2 - du_n^2$$

$$(13) \qquad v_{2n} = v_n^2 - 2$$

$$(14) \qquad 2|u_n \Leftrightarrow 2|v_n \Leftrightarrow 3|n$$

$$(15) \qquad (u_n, v_n) = 1 \quad \text{unless} \quad 3|n$$

$$(16) \qquad (u_n, v_n) = 2 \quad \text{if} \quad 3|n$$

Throughout k will denote an even integer not divisible by 3. Then by (13) and (14) we have

 $v_{n+6} \equiv v_n \pmod{8}$.

$$(18) v_k \equiv 7 \pmod{8}.$$

Also we have using (10)-(13)

(17)

$$\begin{array}{lll} (19) & 2u_{m+2N} \equiv -2u_m \; (\bmod v_N) \\ (20) & 2v_{m+2N} \equiv -2v_m \; (\bmod v_N) \\ (21) & 2v_{m+2N} \equiv & 2v_m \; (\bmod u_N) \\ \text{and so by (18)} & \\ (22) & u_{m+2k} \equiv -u_m \; (\bmod v_k) \\ (23) & v_{m+2k} \equiv -v_m \; (\bmod v_k) \; . \end{array}$$

In particular, taking N=1 in (20) and (21),

(24) if
$$n$$
 is even $v_n \equiv (-1)^{\frac{1}{2}n} 2 \pmod{a}$

(25) if
$$n$$
 is even $v_n \equiv 2 \pmod{b}$.

Thus by (18) and (24) we have

(26)
$$(a | v_k) = (-1 | a)(v_k | a) = ((-1)^{\frac{1}{2}k+1} 2 | a)$$

and by (18) and (25)

$$(27) (b|v_k) = (-1|b)(v_k|b) = (-2|b).$$

Now let $a^2 - 1 = 2^s c$, where c is odd. Then by (21) and (8)

$$2v_k \equiv 2v_{k-6} \equiv \ldots \equiv 2v_{\pm 2} \equiv 2v_2 \pmod{u_3}$$

or, since $c \mid u_3$, $2 \nmid c$

$$\begin{array}{rcl} v_k \equiv v_2 & (\bmod c) \\ & \equiv a^2 - 2 \pmod c \\ & \equiv -1 \pmod c \,. \end{array}$$

Thus,

$$(a^{2}-1|v_{k}) = (2^{s}|v_{k})(c|v_{k})$$

$$= 1 \cdot (-1|c)(v_{k}|c) \quad \text{by (18)}$$

$$= (-v_{k}|c)$$

$$= (1|c)$$

or,

$$(28) (a^2 - 1 | v_k) = 1.$$

Finally we observe that if $2\alpha = a + bd^{\frac{1}{2}}$ is the fundamental solution of $X^2 - dY^2 = 4$, then α^3 is the fundamental solution of $X^2 - dY^2 = 1$, since both a and b are odd. Thus we have the general solution of

(29)
$$X^2 - dY^2 = 4 \text{ is } X = v_n, Y = u_n$$

the general solution of

(30)
$$X^2 - dY^2 = 1$$
 is $X = \frac{1}{2}v_{3n}$, $Y = \frac{1}{2}u_{3n}$.

3. The Fundamental Theorems.

In this section we shall prove four theorems which enable us to say for what values of n, u_n , v_n , $\frac{1}{2}u_n$ and $\frac{1}{2}v_n$ can be perfect squares. In each case the proof is in several parts.

Theorem 1. The equation $v_n = x^2$ has no solutions, except if a is a perfect square, when there are the solutions $n = \pm 1$ and no others.

PROOF. (i) If n is even, by (13)

$$v_n = v_{\frac{1}{2}n}^2 - 2 + x^2.$$

(ii) If $n \equiv 3 \pmod{6}$, then by (17),

$$v_n \equiv v_3 \pmod{8}$$

 $\equiv -2a \pmod{8}$

hence $2|v_n$, $4 \nmid v_n$ and so $v_n \neq x^2$.

(iii) If $n \equiv \pm 1 \pmod{6}$, then by (8) and (17)

$$v_n \equiv v_{+1} \equiv a \pmod{8}$$

and so $v_n \neq x^2$, except possibly if $a \equiv 1 \pmod{8}$.

(iv) If $a \equiv 1 \pmod{8}$ and n is odd, then by (8) it is sufficient to consider only $n \equiv 1 \pmod{4}$. Then if $n \neq 1$ we may write $n = 1 + 2 \cdot 3^r \cdot k$ where $r \geq 0$, $2 \mid k$ and $3 \nmid k$. Then by (23)

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

 $\equiv -a \pmod{v_k}$.

Thus

$$(v_n | v_k) = (-a | v_k)$$

= $-(a | v_k)$ by (18)
= $-(\pm 2 | a)$ by (26)
= -1 since $a \equiv 1 \pmod{8}$.

Hence $v_n \neq x^2$, except possibly for $n = \pm 1$ and this occurs if and only if $a = v_1$ is a perfect square.

This concludes the proof of the theorem.

THEOREM 2. The equation $v_n = 2x^2$ has the solution n = 0, and for d = 725 the solutions $n = \pm 3$, but no other solutions.

PROOF. (i) By (14), $v_n = 2x^2$ is possible only if n = 3m and so we have

$$2x^2 = v_{3m} = v_m(v_m^2 - 3)$$
 by (3) and (4),

and $(v_m, v_m^2 - 3) = 1$ or 3. Now $v_m^2 - 3 = 2x_1^2$ or $3x_1^2$ is impossible as can be seen considering residues modulo 8, and so we have

either
$$v_m^2 - 3 = x_1^2$$
, $v_m = 2x_2^2$;

the former requires $v_m = 2$, which implies n = 0,

$$or \quad v_m^2 - 3 = 6x_1^2, \ v_m = 3x_2^2,$$

where x_2 is odd. Thus we must have $v_m \equiv 3 \pmod{8}$. But, by (8) and (17), if m is even $v_m \equiv v_0$ or $v_2 \pmod{8}$, that is, $v_m \equiv 2$ or $7 \pmod{8}$, which is impossible. If m is odd we have similarly $v_m \equiv v_1 \equiv a \pmod{8}$ (since v_3 is even and v_m is not) and so the only possibility apart from n = 0, is $n \pmod{8}$.

(ii) Suppose now that n is odd and $a \equiv 3 \pmod{8}$. Then as before, it is sufficient to consider only $n \equiv 3 \pmod{4}$. Then if $n \neq 3$ we may write $n = 3 + 2 \cdot 3^r \cdot k$ where $2 \mid k$, $3 \nmid k$. Thus by (23)

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

Now $\frac{1}{2}v_3 \equiv 1 \pmod{4}$ since $a \equiv 3 \pmod{8}$ and so by (20)

$$v_k \equiv -v_{k-6} \equiv \ldots \equiv \pm v_{+2} \equiv \pm v_2 \pmod{\frac{1}{2}v_3}.$$

Thus

$$\begin{array}{ll} (2\,v_n\,|\,v_k) &= \,(-\,2\,v_3\,|\,v_k) \\ &= \,(\frac{1}{2}\,v_3\,|\,v_k) (-\,4\,|\,v_k) \\ &= \,-\,(v_k\,|\,\frac{1}{2}v_3) & \text{by (18)} \\ &= \,-\,(\pm\,v_2\,|\,\frac{1}{2}v_3) \\ &= \,-\,(a^2-2\,|\,\frac{1}{2}(a^2-3)a) \\ &= \,-\,(a^2-2\,|\,a) (a^2-2\,|\,\frac{1}{2}(a^2-3)) \\ &= \,-\,(-\,2\,|\,a) (1\,|\,\frac{1}{2}(a^2-3)) \\ &= \,-\,1 & \text{since } a \equiv 3 \pmod{8} \,. \end{array}$$

Thus $v_n \neq 2x^2$ for n odd, except possibly for $n = \pm 3$ and $a \equiv 3 \pmod{8}$.

(iii) Suppose now that $2x^2=a(a^2-3)=v_{\pm 3}$. Then as before we must have $a=3x_1^2$, $a^2-3=6x_2^2$, or

$$2x_2^2 = 3x_1^4 - 1.$$

Now this equation has by [1] only the positive solutions $x_1 = 1$ or 3, yielding a = 3 or 27. Of these the former must be rejected in view of (9) and we obtain $db^2 = 725$ so that d = 725 or 29. But d = 29 must also be rejected since $x^2 - 29y^2 = -4$ has odd solutions.

This concludes the proof of the theorem. Of course, we could have quoted the result concerning (31) in part (i) of the proof of the theorem, thereby shortening the proof considerably; however, we have sought the best result using only elementary means.

THEOREM 3. The equation $u_n = x^2$ has the solutions

- (a) n = 0
- (b) if $b = B^2$, n = 1
- (c) if $a = A^2$ and $b = B^2$, n = 2
- (d) if $b=3B^2$, possibly the solution n=3

and no other solutions.

PROOF. (i) If $b \equiv 1$ or $3 \pmod 8$ and $n \equiv 1 \pmod 4$. Then if $n \neq 1$ we may write $n = 1 + 2 \cdot 3^r \cdot k$ where $2 \mid k$, $3 \nmid k$. Then by (22)

$$u_n \equiv -u_1 \equiv -b \pmod{v_k}.$$

Thus

$$\begin{aligned} (u_n | v_k) &= (-b | v_k) \\ &= -(b | v_k) & \text{by (18)} \\ &= -(-2 | b) & \text{by (27)} \\ &= -1 & \text{since } b \equiv 1 \text{ or 3 (mod 8)}. \end{aligned}$$

Thus $u_n + x^2$ except possibly for n = 1 in this case. If $u_1 = x^2$, then b is a perfect square.

(ii) If $b \equiv 1$ or 3 (mod 8) and $n \equiv 3 \pmod{4}$, then if $n \neq 3$ we may write $n = 3 + 2 \cdot 3^r \cdot k$ where $2 \mid k$, $3 \nmid k$ and so by (22)

$$u_n \equiv -u_3 \pmod{v_k}$$
.

Thus

$$(u_n|v_k) = (-u_3|v_k)$$

$$= -(b(a^2-1)|v_k) by (18)$$

$$= -(b|v_k)(a^2-1|v_k)$$

$$= -(-2|b) by (27) and (28)$$

$$= -1 since b \equiv 1 \text{ or } 3 \pmod{8}.$$

Thus in this case $u_n + x^2$ except possibly if n = 3. Now $u_3 = b(a^2 - 1) = b(db^2 + 3)$ and so $u_3 = x^2$ implies

either
$$b = x_1^2$$
, $a^2 - 1 = x_2^2$

which is impossible since $a \neq 1$

or
$$b = 3B^2$$
, $a^2 - 1 = 3x_1^2$.

Thus $u_3 = x^2$ is possible only if $b = 3B^2$.

(iii) Now suppose $b \equiv 5$ or 7 (mod 8) and n odd. Then if $n \equiv 1 \pmod{4}$, $u_{-3} < 0$, whereas if $n \neq -3$, let $n = -3 + 2 \cdot 3^r \cdot k$ where $2 \mid k$, $3 \nmid k$. Then by (7) and (22)

$$u_n \equiv -u_{-3} \equiv u_3 \pmod{v_k}.$$

Thus

$$(u_n|v_k) = (u_3|v_k)$$

= $(b|v_k)(a^2-1|v_k)$
= $(-2|b)$ by (27) and (28)
= -1 since $b \equiv 5$ or 7 (mod 8).

Thus $u_n + x^2$ in this case.

Similarly, if $n \equiv 3 \pmod{4}$ then $u_{-1} < 0$ whereas if $n \neq -1$, let $n = -1 + 2 \cdot 3^r \cdot k$ where $2 \mid k, 3 \nmid k$. Then by (7) and (22)

$$u_n \equiv -u_{-1} \equiv b \pmod{v_k}$$
.

Thus

$$(u_n|v_k) = (b|v_k)$$

= $(-2|b)$ by (27)
= -1 since $b \equiv 5$ or 7 (mod 8).

Thus once again $u_n \neq x^2$. This concludes the discussion of n odd.

68 J. H. E. COHN

(iv) Now suppose that n is even and $u_n = x^2$. Then by (10) $x^2 = u_{\frac{1}{2}n}v_{\frac{1}{2}n}$. Thus by (15) and (16) we have

either
$$u_{1n} = x_1^2$$
, $v_{1n} = x_2^2$.

By Theorem 1 the latter is possible only for $\frac{1}{2}n = \pm 1$. The number $\frac{1}{2}n = -1$ does not satisfy the former, and so we have the solution n=2 if and only if $u_1=b$ and $v_1=a$ are both perfect squares,

or
$$u_{\frac{1}{2}n} = 2x_1^2$$
, $v_{\frac{1}{2}n} = 2x_2^2$.

By Theorem 2 the latter can be satisfied only for n=0, 6 and -6. Of these values the first always satisfies the former equation and the last never. If n=6 we should have to have $u_3=2x_1^2$, $v_3=2x_2^2$. By Theorem 2 the latter can only hold for d=725 and for this value $u_3=728 \pm 2x_1^2$.

This concludes the proof of the theorem.

Theorem 4. The equation $u_n = 2x^2$ has

- (a) the solution n=0
- (b) if $b = B^2$ possibly the solution n = 3

and no other solutions.

PROOF. (i) Since by (18) $(2|v_k)=1$, it follows exactly as in the proof of Theorem 3, that with the exception of n=1 or 3 and $b\equiv 1$ or 3 (mod 8), for each odd n we can find k such that $(2u_n|v_k)=-1$ and so $u_n \neq 2x^2$.

Also $u_1 = b + 2x^2$, and so the only possibility for odd n is n = 3. Now if $2x^2 = u_3 = b(a^2 - 1) = b(db^2 + 3)$, then we must have

either
$$b = 3x_1^2$$
, $db^2 + 3 = 6x_2^2$, $3dx_1^4 = 2x_2^2 - 1$,

which is impossible as is seen by considering residues modulo 3,

or
$$b = x_1^2$$
, $a^2 - 1 = 2x_2^2$.

This concludes the discussion of n odd.

(ii) Now suppose that n is even. Then if $u_n = 2x^2$ it follows from (14) that $3 \mid n$. Also by (10) $2x^2 = u_{\frac{1}{2}n}v_{\frac{1}{2}n}$ and so by (15) and (16) we must have

either
$$u_{1n} = 2x_1^2$$
, $v_{1n} = x_2^2$

which is impossible for n divisible by 3, by Theorem 1,

or
$$u_{\frac{1}{2}n} = x_1^2$$
, $v_{\frac{1}{2}n} = 2x_2^2$.

Now by Theorem 2 the latter is satisfied by $\frac{1}{2}n = 0$ and also if d = 725 by $\frac{1}{2}n = \pm 3$. Now $\frac{1}{2}n = 0$ satisfies the former, and if d = 725, $u_{\pm 3} = \pm 728 \pm x_1^2$.

This concludes the proof.

4. The Equations.

As a corollary to the results of \S 3, we now deduce some results concerning the following Diophantine equations. Of course d is restricted to the values mentioned in the introduction. We consider only non-negative solutions.

Equation 1. $y^2 = dx^4 + 1$ has apart from x = 0 at most one solution.

For, by (30), $x^2 = \frac{1}{2}u_{3n}$, and so by Theorem 4, we have n = 0 yielding x = 0 and possibly n = 1.

Equation 2. $dy^2 = x^4 - 1$ has the solution x = 1 and, except for d = 725, x = 99, no other.

For, by (30), $x^2 = \frac{1}{2}v_{3n}$, and so by Theorem 2, the result follows.

Equation 3. $y^2 = 4dx^4 + 1$ has apart from x = 0 at most one solution.

For, by (30), $2x^2 = \frac{1}{2}u_{3n}$, i.e. $u_{3n} = (2x)^2$. This has the solution n = 0, yielding x = 0, and by Theorem 3 it may also have the solution n = 1.

Equation 4. $y^2 = dx^4 + 4$ has apart from x = 0 at most two solutions.

For, by (29), $x^2 = u_n$. By Theorem 3, this is satisfied by n = 0 which gives x = 0, and by at most two of the values n = 1, 2, and 3.

Equation 5. $dy^2 = x^4 - 4$ has at most one solution.

For, by (29), $x^2 = v_n$ and by Theorem 1, this can only be satisfied by $n = \pm 1$, giving $x = a^{\frac{1}{2}}$.

For the sake of completeness, we should like to point out that the six equations

$$dy^2 = 4x^4 + 1,$$
 $dy^2 = x^4 + 1,$
 $y^2 = dx^4 - 1,$ $dy^2 = 4x^4 - 1,$
 $y^2 = dx^4 - 4,$ $dy^2 = x^4 + 4$

all have no solutions for the values of d considered. This may be shown similarly to those above, or deduced by simple modulus arguments combined with (1) and (2). We observe that our method together with that of [2] deals with all values less than 200 of $d \equiv 5 \pmod{8}$ except 37, 101, 141, 189 and 197.

5. A Different Approach.

Until now, we have generally assumed that d is given first, and that a and b and thus all the u_n and v_n are determined from d. Let us now

consider an odd value, x, of a. Then if we take $d=x^2-4$, we see that the equation $X^2-dY^2=4$ has odd solutions, since one of them is X=x, Y=1. It is clear that this is the fundamental solution. Moreover, provided $x \ge 5$, it may be shown without difficulty that the equation $X^2-dY^2=-4$ has no solutions. Thus there are infinitely many values of d which satisfy our condition, and we may choose for a any odd value $x \ge 5$, and b=1. Thus as in [1], we may define polynomials $p_n(x)$ and $q_n(x)$ of degrees (n-1) and n respectively, by the relations

(32)
$$p_0(x) = 0$$
, $p_1(x) = 1$, $q_0(x) = 2$, $q_1(x) = x$

(33)
$$p_{n+2}(x) = x p_{n+1}(x) - p_n(x)$$

$$q_{n+2}(x) = xq_{n+1}(x) - q_n(x)$$

and then we obtain immediately from Theorems 1-4 four results of which the following is typical: "The equation $y^2 = p_n(x)$ has for $n \ge 3$ no solutions in which $x \ge 5$ is odd." We may ask about the values x = 1, x = 3. Now for x = 1, the problem is trivial since it can easily be seen that $p_n(1)$ and $q_n(1)$ can take only the values $0, \pm 1$ and $+1, \pm 2$ respectively. For x = 3, we can easily show that $p_n(3) = F_{2n}$ and $q_n(3) = L_{2n}$ where F_n, L_n are respectively the Fibonacci and Lucas numbers. Thus using Theorems 1-4 and the results in [3] we obtain

THEOREM 5. The equation $y^2 = p_n(x)$ has for $n \ge 3$ no solution in which $x \ge 3$ is odd, except x = 3, y = 12, n = 6.

THEOREM 6. The equation $2y^2 = p_n(x)$ has for n > 3 no solution in which $x \ge 3$ is odd.

THEOREM 7. The equation $y^2 = q_n(x)$ has for n > 1 no solution in which $x \ge 3$ is odd.

THEOREM 8. The equation $2y^2 = q_n(x)$ has for n > 0 no solution in which $x \ge 3$ is odd, except x = 3, y = 3, n = 3 and x = 27, y = 99, n = 3.

REFERENCES

- 1. Richard T. Bumby, The Diophantine equation $3x^4-2y^2=1$, Math. Scand. 21 (1967), 144-148.
- J. H. E. Cohn, Eight Diophantine equations, Proc. Lond. Math. Soc. (3) 16 (1966), 153-166.
- 3. J. H. E. Cohn, Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Ass. 7 (1965), 24-29.

BEDFORD COLLEGE, LONDON, N. W. 1., ENGLAND

AND

UNIVERSITY OF CALIFORNIA, LOS ANGELES, U.S.A.