PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 2, 1968

SOME QUARTIC DIOPHANTINE EQUATIONS

J. H. E. COHN

Elementary methods are used to solve some quartic Diophantine equations, of which $x^2 = dy^4 + m$ is typical, where m is an integer, positive or negative and d is a positive integer with the property that the equation $x^2 - dy^2 = 4$ has at least one solution x, y where both x and y are odd.

The cases $m = \pm 1, \pm 4$ have been treated previously and in these cases the equations have been solved completely. The object here is to try to extend the method to cover all other values of m. In view of the greater generality of the problem, it is not surprising that the theorems obtained are weaker. However, the method does give a complete solution of the problem in many cases.

In the first place, let us consider the admissible values of d. Clearly if $x^2 - dy^2 = 4$ is to have a solution with x and y both odd, it is necessary that $d \equiv 5 \pmod 8$. Unfortunately this condition is not sufficient, there are five values $d = 37, 101, 141, 189$ and 197 less than 200 which satisfy it without the equation having any odd solutions. There is no simple known necessary and sufficient condition, although several sufficient conditions are known, and these do guarantee the existence of infinitely many such d.

Secondly suppose that $x^2 - dy^2 = 4$ does have a solution in which both x and y are odd. What can be said about the equation $x^2 - dy^2 = -4$? It is easily shown [see 2; § 2] that this will possess a pair of solutions x, y both of which are odd if $x^2 - dy^2 = -1$ has *any* solutions, and none at all otherwise. Again no simple necessary and sufficient conditions are known for the existence of solutions of $x^2 - dy^2 = -1$; it is clearly necessary that d have no factor $\equiv 3 \pmod 4$, and it is known to be sufficient that d be a prime $\equiv 1 \pmod 4$. The main part of this paper will be divided into two parts; in the first we suppose that $x^2 - dy^2 = -4$ has at least one pair of solutions both of which are odd; in the second we suppose that $x^2 - dy^2 = -4$ has no solutions but that $x^2 - dy^2 = 4$ has at least one such set of solutions.

1. We suppose here that $x^2 - dy^2 = -4$ has a pair of solutions x, y both of which are odd. Such values of d have been considered in [1], and we shall use the notation and results from [1]. Thus if the fundamental solution of $x^2 - dy^2 = -4$ is $2\alpha = a + b\sqrt{d}$, then a and b are both odd and 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; we have $2\beta = a - b\sqrt{d}$, $u_n\sqrt{d} = \alpha^n - \beta^n$ and $v_n = \alpha^n + \beta^n$.

Now consider the equation $x^2 - dy^2 = m$. Of course there are values of m for which this has no solutions at all; for example $x^2 - 5y^2 = 7$ can have no solution as it cannot even be satisfied modulo 5. Again however no simple set of sufficient conditions exists; thus $x^2 - 229y^2 = 3$ has no solutions although it possesses solutions in p-adic integers for every prime p.

Now suppose that $x^2 - dy^2 = m$ possesses solutions. Since $d \equiv 5 \pmod 8$ it follows that if m is even, the factor 2 occurs in m raised to an even power. Suppose first that $16 | m$. Then since $d \equiv 5 \pmod 8$, both x and y must be even for any solution and so

$$\left(\frac{1}{2}x\right)^2 - d\left(\frac{1}{2}y\right)^2 = \frac{1}{4}m .$$

If $(1/4)m$ is still divisible by 16 we may proceed in like fashion. Thus to find the solutions of $x^2 - dy^2 = m$ it is sufficient to consider only values of m that are odd, or are odd multiples of 4.

In the following, let m be any odd integer. Then the four equations

$$x^2 - dy^2 = m,\ x^2 - dy^2 = 4m,\ x^2 - dy^2 = -m \quad \text{and} \quad x^2 - dy^2 = -4m ,$$

either all have solutions *or* none has solutions. For if $x + y\sqrt{d}$ is a solution of $x^2 - dy^2 = m$, then the other three equations have respectively the solutions

$$2(x + y\sqrt{d});\ (x + y\sqrt{d})\alpha^3 \quad \text{and} \quad 2(x + y\sqrt{d})\alpha^3 .$$

Conversely if $x + y\sqrt{d}$ is a solution of $x^2 - dy^2 = 4m$, then since d is odd, x and y are either both even or both odd; if both even then $1/2(x + y\sqrt{d})$ is a solution of $x^2 - dy^2 = m$ and the other solutions follows as before, whereas if both are odd then exactly one of

$$(x + y\sqrt{d})\alpha^2 \quad \text{and} \quad (x + y\sqrt{d})\beta^2$$

which are both solutions of $x^2 - dy^2 = 4m$ has both 'x' and 'y' even, since

$$(x + y\sqrt{d})\alpha^2 + (x + y\sqrt{d})\beta^2 = (x + y\sqrt{d})(\alpha^2 + \beta^2) = (x + y\sqrt{d})v_2$$

and x, y, v_2 are all odd. The other cases follow similarly.

We now suppose, in view of the previous remarks, that m is an odd positive integer and that $x^2 - dy^2 = m$ has solutions. Then as is well known the totality of solutions of this equation is contained in a finite number of classes $K_1, K_2, \cdots, K_r$ and the conjugate classes $K_1^*, K_2^*, \cdots, K_r^*$, some of which may be ambiguous; see for example

[3; p. 207]. In what follows, except in Theorem 1.1, each class must be taken separately and we shall assume that we are considering only one given class K. As a matter of fact, all the solutions in the conjugate class K^* differ from those in K only in order and the signs of x and y which occur, and so we can eliminate discussion of K^*.

Consider now the fundamental solution of $x^2 - dy^2 = m$ in the class considered. Let it be $1/2(s_0 + t_0\sqrt{d})$ and define for each integer n,

$$s_n + t_n\sqrt{d} = (s_0 + t_0\sqrt{d})\alpha^n .$$

Then s_0 and t_0 are both even and it is easily seen that the general solution of the equation

$$\begin{array}{lll} x^2 - dy^2 = 4m & \text{is} & \pm s_{2n} \pm t_{2n}\sqrt{d} \\ \text{of } x^2 - dy^2 = -4m & \text{is} & \pm s_{2n+1} \pm t_{2n+1}\sqrt{d} \\ \text{of } x^2 - dy^2 = m & \text{is} & \frac{1}{2}(\pm s_{6n} \pm t_{6n}\sqrt{d}) , \\ \text{and of } x^2 - dy^2 = -m & \text{is} & \frac{1}{2}(\pm s_{6n+3} \pm t_{6n+3}\sqrt{d}) . \end{array}$$

(These are the solutions obtained from a class K and its conjugate K^*; if there are more classes, they will provide more solutions of the same type.) It follows that to determine the solutions of, say, $x^2 = dy^4 + m$, we must find for what values of n if any $t_{6n} = \pm 2y^2$. We shall therefore be interested in determining for what n it is possible that either s_n or t_n equals hx^2 where $h = 1, -1, 2$ or -2. Unlike the simple case $m = 1$, it will not be possible to establish theorems which completely determine the possible n in all the cases that can arise. We shall however indicate methods which often enable the complete solution to be determined in any given case.

THEOREM 1.1. *If m, d have no common factor $\equiv 5 \pmod 8$ then either* (*a*) $s_{6n} \neq \pm 2x^2$ *and* $s_{2n+1} \neq \pm x^2$ *for any n, K or* (*b*) $s_{6n+3} \neq \pm 2x^2$ *and* $s_{2n} \neq \pm x^2$ *for any n, K or possibly both.*

Proof. Since $d \equiv 5 \pmod 8$ and d has only factors $\equiv 1 \pmod 4$ it follows that d has at least one prime factor $p \equiv 5 \pmod 8$. Suppose now that (a) is false, say for example that $s_{6n} = \pm 2x^2$ for some n, K. Then the equation $x^4 - dy^2 = m$ has at least one solution and in particular the congruence

$$x^4 \equiv m \pmod p \tag{1.1}$$

is solvable. Now since $(m, d) = 1$ it follows that $p \nmid m$ and so a solution of (1.1) satisfies

$$x^2 \equiv \pm m_1 \pmod{p} \tag{1.2}$$

where therefore $(m_1 \mid p) = 1$, and so

$$m_1^{\frac{1}{2}(p-1)} \equiv 1,\ m \equiv m_1^2 \pmod{p}\ . \tag{1.3}$$

It now follows that $x^4 - dy^2 = 4m$ is impossible; for it would require $x^4 \equiv 4m \pmod{p}$, hence $x^2 = \pm 2m_1 \pmod{p}$ which is impossible since

$$(\pm 2m_1 \mid p) = (2 \mid p)(m_1 \mid p) = -1$$

since $p \equiv 5 \pmod{8}$. Similarly $x^4 - dy^2 = -m$ is impossible since it would require $x^4 \equiv -m \pmod{p}$ and so

$$\begin{aligned} x^{p-1} = (x^4)^{\frac{1}{4}(p-1)} &\equiv (-m)^{\frac{1}{4}(p-1)} \\ &\equiv (-1)^{\frac{1}{4}(p-1)} m_1^{\frac{1}{2}(p-1)} \\ &\equiv -1 \qquad\qquad \pmod{p} \end{aligned}$$

using (1.3), since $p \equiv 5 \pmod{8}$, which is of course impossible. Thus neither $x^4 - dy^2 = 4m$ nor $x^4 - dy^2 = -m$ has any solutions and so for all n and K both $s_{6n+3} = \pm 2x^2$ and $s_{2n} = \pm x^2$ are impossible.

The other cases of the theorem may be proved in like fashion.

This theorem has the advantage over the other methods below in that it deals simultaneously with all classes K. However, it applies only to s_n and connot be extended to t_n.

From the definition we have

$$\begin{aligned} s_n + t_n\sqrt{d} &= (s_0 + t_0\sqrt{d})\alpha^n \\ s_n - t_n\sqrt{d} &= (s_0 - t_0\sqrt{d})\beta^n\ . \end{aligned}$$

Thus using the notation of [1]

$$\begin{aligned} 2s_n &= s_0(\alpha^n + \beta^n) + t_0(\alpha^n - \beta^n)\sqrt{d} \\ &= s_0 v_n + dt_0 u_n \end{aligned}$$

or

$$s_n = \left(\frac{1}{2}s_0\right)v_n + \left(\frac{1}{2}dt_0\right)u_n \tag{1.4}$$

and similarly

$$t_n = \left(\frac{1}{2}t_0\right)v_n + \left(\frac{1}{2}s_0\right)u_n \,. \tag{1.5}$$

It therefore follows from [1 (15)] and the corresponding result for u_n that

$$s_{n+12} \equiv s_n \pmod 8 \tag{1.6}$$

and

$$t_{n+12} \equiv t_n \pmod 8 \,. \tag{1.7}$$

It may also be shown that

$$s_{n+12} \equiv s_n \pmod{16} \quad \text{if } 3 \mid n \tag{1.8}$$

and

$$t_{n+12} \equiv t_n \pmod{16} \quad \text{if } 3 \mid n \,. \tag{1.9}$$

These equations together with an evaluation of the first twelve values of s_n and t_n enable a preliminary statement to be made about possible values of n for which s_n or t_n can equal hx^2; it is usually possible to eliminate a considerable number of residue classes modulo 12 in each case. Actually the sequences $\{s_n\}$ and $\{t_n\}$ are periodic modulo any integer and this often provides extra information by a suitable choice of modulus.

In the following $k = 2^r$ where r is a positive integer. This is a slight departure from the notation of [1] for there k was only supposed to satisfy $2 \mid k$, $3 \nmid k$. Then using formulae (4), (5), (16), (22) and (23) of [1] and our (1.4) and (1.5) we have

$$s_{n+2k} \equiv -s_n \pmod{v_k} \tag{1.10}$$

$$t_{n+2k} \equiv -t_n \pmod{v_k} \tag{1.11}$$

$$v_2 \equiv 3 \pmod 8 \tag{1.12}$$

$$v_k \equiv 7 \pmod 8 \,, \quad \text{if} \quad k = 2^r \quad \text{and } r \geqq 2 \tag{1.13}$$

$$s_{n+2} = as_{n+1} + s_n \tag{1.14}$$

$$t_{n+2} = at_{n+1} + t_n \,. \tag{1.15}$$

We now prove

THEOREM 1.2. *If* $h = \pm 1$ *or* ± 2, $k = 2^r$ *where* $r \geqq 1$ *and if* $(t_n, v_k) = 1$ *and* $(ht_n \mid v_k) = 1$, *then*

(a) $t_N \neq hy^2$ *for* $N \equiv n + 2k \pmod{4k}$

(b) $t_N \neq -hy^2$ *for* $N \equiv n \pmod{4k}$

(c) $t_N \neq \dfrac{2}{h}y^2$ *for* $N \equiv n + 2k \pmod{4k}$ *if* $r \geqq 2$

(d) $t_N \neq -\dfrac{2}{h}y^2$ *for* $N \equiv n \pmod{4k}$ *if* $r \geqq 2$

(e) $t_N \neq -\dfrac{2}{h}y^2$ *for* $N \equiv n + 4 \pmod{8}$ *if* $r = 1$

(f) $t_N \neq \dfrac{2}{h}y^2$ *for* $N \equiv n \pmod{8}$ *if* $r = 1$,

with a similar set of results for s. In particular the result follows if $t_n = hy_1^2$ *and* $(t_n, v_k) = 1$.

Proof. (i) Let $N \equiv n + 2k \pmod{4k}$. Then $N = n + 2kl$ where l is odd and so by (1.11)

$$\begin{aligned} t_N &= t_{n+2kl} \\ &\equiv (-1)^l t_n \pmod{v_k} \\ &\equiv -t_n \pmod{v_k}\,. \end{aligned}$$

Thus

$$(ht_N \mid v_k) = (-ht_n \mid v_k) = (-1 \mid v_k) = -1 \quad \text{by (1.12) and (1.13)}$$

$$\left(\frac{2}{h}t_N \mid v_k\right) = (-2ht_n \mid v_k) = (-2 \mid v_k) = -1 \quad \text{by (1.13) if } r \geqq 2$$

and

$$\left(-\frac{2}{h}t_N \mid v_2\right) = (2ht_n \mid v_2) = (2 \mid v_2) = -1 \qquad \text{by (1.12) if } r = 1$$

and this proves (a), (c) and (e).

(ii) Let $N \equiv n \pmod{4k}$. Then $N = n + 2kL$ where L is even and so by (1.11)

$$\begin{aligned} t_N &= t_{n+2kL} \\ &\equiv (-1)^L t_n \pmod{v_k} \\ &\equiv t_n \pmod{v_k}\,. \end{aligned}$$

Then (b), (d) and (f) follow in exactly similar fashion. The proof for s is exactly similar, using (1.10).

THEOREM 1.3. *If* $h = \pm 1$ *or* ± 2 *and if* $(t_n, v_k) = 1$ *and* $(ht_n \mid v_k) = 1$ *for all* $k = 2^r$ *with* $r \geqq R$, *then*

(a) $t_N \neq hy^2$ *for* $N \equiv n \pmod{2^{R+1}}$, $N \neq n$

(b) $t_N \neq -hy^2$ *for* $N \equiv n \pmod{2^{R+2}}$

(c) $t_N \neq \frac{2}{h}y^2$ *for* $N \equiv n \pmod{2^{R+1}}$, $N \neq n$ *if* $R \geqq 2$

(d) $t_N \neq -\frac{2}{h}y^2$ *for* $N \equiv n \pmod{2^{R+2}}$ *if* $R \geqq 2$

(e) $t_N \neq \frac{2}{h}y^2$ *for* $N \equiv n \pmod{8}$ *if* $R = 1$

(f) $t_N \neq -\frac{2}{h}y^2$ *for* $N \equiv n \pmod{16}$ *or* $N \equiv n + 4 \pmod{8}$

if $R = 1$, *with analogous results for* s.

Proof. (i) If $N \equiv n \pmod{2^{R+1}}$, $N \neq n$, then $(N - n)$ is a nonzero integer divisible by 2^{R+1}. Suppose that 2^{R+p+1} is the highest power of 2 which divides $(N - n)$ where $p \geqq 0$. Then if $k = 2^{R+p}$, $N - n \equiv 2k \pmod{4k}$ and (a) and (c) follow from parts (a) and (c) of Theorem 1.2.

(ii) If $N \equiv n \pmod{2^{R+2}}$, then if $k = 2^R$, $N \equiv n \pmod{4k}$ and (b) and (d) follow from parts (b) and (d) of Theorem 1.2.

(iii) Now Suppose that $R = 1$. Then we may apply Theorem 1.2 (f) to obtain (e). To prove (f) we may use Theorem 1.2 (d) with $r = 2$ and Theorem 1.2 (e) with $r = 1$. This concludes the proof.

It might be thought that the usefulness of these results might be limited by the difficulty of ensuring that a given s_n (or t_n) has no factor in common with any of the v_k, and by the difficulty of calculating $(hs_n \mid v_k)$ for the various values of k. This however is not the case for by [1 (11)], we see that if $k = 2^r$, $v_{2k} = v_k^2 - 2$ and so the residues of the sequence $\{v_k\}$ modulo any integer form a sequence which is eventually periodic. It is thus fairly simple to find out whether a given s_n has any factors in common with any v_k. Of course, sometimes it does happen that $(s_n, v_k) \neq 1$ and in these cases, further discussion is necessary.

To illustrate the method, we append a detailed discussion of an example, which displays most of the above points.

EXAMPLE. Consider the case $d = 5, m = 11$. Then $a = b = 1$, the fundamental solution of $x^2 - dy^2 = 1$ is $\alpha^6 = 9 + 4\sqrt{5}$ and so using the method of [3], p. 205, it is seen that the equation $x^2 - 5y^2 = 11$ has only the class of solutions whose fundamental solution is $4 + \sqrt{5}$, and the conjugate class. Thus $s_0 = 8$, $t_0 = 2$ and we obtain the following table of values

n	s_n	mod 8	mod 16	t_n	mod 8	mod 16
-6	32	0	0	-14	2	2
-5	-19	5		9	1	
-4	13	5		-5	3	
-3	-6	2	10	4	4	4
-2	7	7		-1	7	
-1	1	1		3	3	
0	8	0	8	2	2	2
1	9	1		5	5	
2	17	1		7	7	
3	26	2	10	12	4	12
4	43	3		19	3	
5	69	5		31	7	
6	112	0	0	50	2	2
7	181			81		

We observe that Theorem 1.1 is applicable in this case; since $s_0 = 2\cdot 2^2$, we see that $s_{2n} \neq \pm x^2$ and $s_{6n+3} \neq \pm 2x^2$. Combining this with the results obtained by using (1.6)-(1.9) we obtain

(A) $s_n = x^2$ implies $n \equiv 1$ or $11 \pmod{12}$

(B) $s_n = -x^2$ is impossible

(C) $s_n = 2x^2$ implies $n \equiv 0$ or $6 \pmod{12}$

(D) $s_n = -2x^2$ implies $n \equiv 0$ or $6 \pmod{12}$

(E) $t_n = y^2$ implies $n \equiv 7$ or $9 \pmod{12}$

(F) $t_n = -y^2$ implies $n \equiv 2, 3, 5$ or $10 \pmod{12}$

(G) $t_n = 2y^2$ implies $n \equiv 0$ or $6 \pmod{12}$

(H) $t_n = -2y^2$ is impossible.

We now consider these possibilities in turn.

Since $s_{-1} = 1^2$, it follows from Theorem 1.3, that $n = -1$ is the only $n \equiv 11 \pmod{12}$ for which $s_n = x^2$. Also $s_1 = 3^2$ and since $3 \nmid v_k$ if $k = 2^r$ and $r \geqq 2$, it follows that $s_n \neq x^2$ if $n \equiv 1 \pmod 8$ and $n \neq 1$. Also $s_{13} = 3249 = 57^2$. Now $57 = 3.19$ and so modulo 19 we find the residues of $\{v_k\}$; they are $3, 7, 9, 3, 7, 9, \cdots$ and so $19 \nmid v_k$ for any $k = 2^r$. Thus $(s_{13}, v_k) = 1$ if $k = 2^r$ and $r \geqq 2$. Thus $s_n \neq x^2$ if $n \equiv 13 \pmod 8$ and $n \neq 13$. Thus we have

$$s_n \neq -x^2;\ s_n = x^2 \textit{ if and only if } n = -1, 1 \textit{ or } 13\ .$$

Since $s_0 = 2\cdot 2^2$, it follows that $s_n = 2x^2$ and $n \equiv 0 \pmod 4$ is possible only for $n = 0$; similarly since $s_{-6} = 2\cdot 4^2$, $n = -6$ is the only $n \equiv 2 \pmod 4$ for which $s_n = 2x^2$. It follows from (C) that $n = 0, -6$ are the only values for which $s_n = 2x^2$. Regarding $s_n = -2x^2$, we see from (D) that n would have to be even, and it is easily seen that s_n is positive for such n. Thus

$$s_n \neq -2x^2;\ s_n = 2x^2 \textit{ if and only if } n = 0 \textit{ or } -6 .$$

Now consider $t_n \cdot t_{-3} = 2^2$ and so $n = -3$ is the only $n \equiv 1 \pmod 4$ for which $t_n = y^2$. Just as before $t_{-5} = 3^2$ and $t_7 = 9^2$ give the only cases of $t_n = y^2$ with $n \equiv 3 \pmod 4$. Since $t_{-2} = -1^2$, $t_n \neq -y^2$ for $n \equiv 2 \pmod 4$, $n \neq 2$. Other even values of n are excluded by (F) and odd values are impossible, since as is easily shown, $t_n > 0$ if n is odd. Thus

$$t_n = y^2 \textit{ if and only if } n = -5, -3 \textit{ or } 7;\ t_n = -y^2$$
$$\textit{if and only if } n = -2 .$$

Finally, $t_n = 2y^2$ is only possible for even n; since $t_0 = 2$ and $t_6 = 2\cdot 5^2$ and since $5 \nmid v_k$ for any $k = 2^r$ we see that, using (H).

$$t_n \neq -2y^2;\ t_n = 2y^2 \textit{ if and only if } n = 0 \textit{ or } 6 .$$

Summarizing these results, we have (listing only positive solutions in each case):

(i) The equation $x^4 = 5y^2 - 44$ has only the solutions (1, 3), (3, 5) and (57, 1453).

(ii) The equation $x^4 = 5y^2 + 11$ has only the solutions (2, 1) and (4, 7).

(iii) The equation $x^2 = 5y^4 + 44$ has only the solution (7, 1).

(iv) The equation $x^2 = 5y^4 + 11$ has only the solutions (4, 1) and (56, 5).

(v) The equation $x^2 = 5y^4 - 44$ has only the solutions (6, 2), (19, 3) and (181, 9).

2. We now consider values of d for which $x^2 - dy^2 = -4$ does not have solutions, but $x^2 - dy^2 = 4$ does have a solution for which both x and y are odd. Although the results are broadly similar to those of the previous case, there are some significant differences, and we shall point these out and state results without detailed proofs. The notation is now that of [2]. Thus $2\alpha = a + b\sqrt{d}$, the fundamental solution of $x^2 - dy^2 = 4$, and β, u_n and v_n are defined as before.

As before in considering $x^2 - dy^2 = m$ it is sufficient to assume that m is either odd or an odd multiple of 4. For any odd m, it may be shown just as before that the two equations $x^2 - dy^2 = m$

and $x^2 - dy^2 = 4m$ either both have solutions, or neither has solutions. However, unlike the previous case there is no special connection between $x^2 - dy^2 = m$ and $x^2 - dy^2 = -m$; indeed it usually happens that when one of these has solutions, the other does not. It might thought that this always happens, for in the case we consider $x^2 - dy^2 = -1$ has no solutions, but this is not so; $d = 221$ is a value which satisfies all our conditions and yet both $x^2 - 221y^2 = 25$ and $x^2 - 221y^2 = -25$ have solutions, namely (5, 0) and (14, 1) respectively. In any case the equations $x^2 - dy^2 = m$ and $x^2 - dy^2 = -m$ must be considered separately. We thus consider $x^2 - dy^2 = m$ where m is an odd integer, positive or negative.

As before let K be one of the classes $K_1, K_2, \cdots, K_r$ of solutions of $x^2 - dy^2 = m$. Then if $1/2(s_0 + t_0\sqrt{d})$ is the fundamental solution in K we define as before $s_n + t_n\sqrt{d} = (s_0 + t_0\sqrt{d})\alpha^n$, and again we wish to determine the possible n for which s_n or t_n equals hx^2 where $h = \pm 1$ or ± 2.

Care is required in the statement of a theorem parallel to Theorem 1.1; as it stands the theorem is false in this case, since for example both the equations $x^4 - 21y^2 = -5$ and $x^4 - 21y^2 = -20$ possess solutions. The reason is that in the proof we require d to have a prime factor $p \equiv 5 \pmod 8$ which does not also divide m. In the first part, the existence of such a factor was assured; in this part, d may not have any such factor at all. However, if this proviso is made, we obtain in just the same manner.

THEOREM 2.1. *If d has a prime factor $p \equiv 5 \pmod 8$ and $p \nmid m$ then*
either (a) $s_n \neq \pm x^2$ *for any* n, K
or (b) $s_{3n} \neq \pm 2x^2$ *for any* n, K
or possibly both.

We obtain, just as before, in the notation of [2]

$$s_n = \left(\frac{1}{2}s_0\right)v_n + \left(\frac{1}{2}dt_0\right)u_n \tag{2.1}$$

$$t_n = \left(\frac{1}{2}t_0\right)v_n + \left(\frac{1}{2}s_0\right)u_n \tag{2.2}$$

$$s_{n+6} \equiv s_n \pmod 8 \tag{2.3}$$

$$t_{n+6} \equiv t_n \pmod 8 \tag{2.4}$$

$$s_{n+6} \equiv s_n \pmod{16} \quad \text{if } 3 \mid n \tag{2.5}$$

$$t_{n+6} \equiv t_n \pmod{16} \quad \text{if } 3 \mid n \tag{2.6}$$

$$s_{n+2k} \equiv -s_n \pmod{v_k} \quad \text{if } k = 2^r \tag{2.7}$$

$$t_{n+2k} \equiv -t_n \pmod{v_k} \quad \text{if } k = 2^r \tag{2.8}$$

$$v_k \equiv 7 \pmod{8} \quad \text{if } k = 2^r \tag{2.9}$$

$$s_{n+2} = as_{n+1} - s_n \tag{2.10}$$

$$t_{n+2} = at_{n+1} - t_n \,. \tag{2.11}$$

It will be observed that (2.9) differs slightly from the corresponding (1.12) and (1.13), and this will slightly simplify the remaining theorems. We obtain

THEOREM 2.2. *If* $h = \pm 1$ *or* ± 2, $k = 2^r$ *where* $r \geqq 1$ *and if* $(t_n, v_k) = 1$ *and* $(ht_n \mid v_k) = 1$, *then*

(a) $t_N \neq hy^2$ *for* $N \equiv n + 2k \pmod{4k}$

(b) $t_N \neq -hy^2$ *for* $N \equiv n \pmod{4k}$

(c) $t_N \neq \frac{2}{h}y^2$ *for* $N \equiv n + 2k \pmod{4k}$

(d) $t_N \neq -\frac{2}{h}y^2$ *for* $N \equiv n \pmod{4k}$

with a similar result for s.

THEOREM 2.3. *If* $h = \pm 1$ *or* ± 2 *and if* $(t_n, v_k) = 1$ *and* $(ht_n \mid v_k) = 1$ *for all* $k = 2^r$ *with* $r \geqq R$, *then*

(a) $t_N \neq hy^2$ *for* $N \equiv n \pmod{2^{R+1}}$, $N \neq n$

(b) $t_N \neq -hy^2$ *for* $N \equiv n \pmod{2^{R+2}}$

(c) $t_N \neq \frac{2}{h}y^2$ *for* $N \equiv n \pmod{2^{R+1}}$, $N \neq n$

(d) $t_N \neq -\frac{2}{h}y^2$ *for* $N \equiv n \pmod{2^{R+2}}$

with a similar result for s.

REFERENCES

1. J. H. E. Cohn, *Eight Diophantine equations*, Proc. Lond. Math. Soc. (3) **16** (1966), 153-166.

2. ———, *Five Diophantine equations*, Math. Scand. **21** (1968) (to appear)

3. T. Nagell, *Introduction to Number Theory*, Uppsala, 1951.

Received May 17, 1967.

ROYAL HOLLOWAY COLLEGE, ENGLEFIELD GREEN, SURREY AND
UNIVERSITY OF CALIFORNIA, LOS ANGELES