ACTA ARITHMETICA
LXXVIII.4 (1997)

The Diophantine equation $x^4 - Dy^2 = 1$, II

by

J. H. E. Cohn (London)

Over fifty years ago, Ljunggren [7] showed that the equation of the title has at most two solutions in positive integers for any fixed D, without loss of generality assumed square free. The method was purely algebraic, but rather complicated. He furthermore stated that $D = 1785$ was the only case known to him when there were actually two solutions, and also claimed to be able to find the solutions when they existed by a finite algorithm; this statement whilst technically true is not as useful as might appear, for although *when there are two solutions* these can be found by his method, the method apparently provided no general way in which when there are not two solutions the fact could be demonstrated.

Progress since then has been in two directions. On the one hand, attempts have been made to find simpler, indeed technically elementary, methods of attacking the problem; these have to date yielded results only for special, albeit infinite, sets of values of D. Thus it has been shown ([1]–[3]) that there are no solutions if either of the equation $X^2 - DY^2 = \pm 4$ has solutions with X and Y both odd with the exceptions $D = 5$ and 29, nor [4] excluding $D = 6$, if either of the equation $X^2 - DY^2 = \pm 2$ has solutions.

In a quite different direction, analytical methods of great depth have recently been used to prove that provided D is sufficiently large, there is at most one solution. The best result of which I am aware appears to be that of [5] which proves that there is at most one solution if $D \geq 9.379 \cdot 10^8$.

Combining an idea of [5] with Ljunggren's result we prove the

Theorem. *Let the fundamental solution of the equation $v^2 - Du^2 = 1$ be $a + b\sqrt{D}$. Then the only possible solutions of the equation of the title are given by $x^2 = a$ and $x^2 = 2a^2 - 1$; both solutions occur in only one case, $D = 1785$.*

Proof. Let $\alpha = a + b\sqrt{d}$ and $\beta = a - b\sqrt{d}$. Then for a solution we must have for some positive integer m, $x^2 = \frac{1}{2}(\alpha^m + \beta^m) = v_m$, say. Since $\alpha + \beta = 2a$, $\alpha\beta = 1$, the sequence $\{v_m\}$ satisfies the recurrence $v_{m+2} =$

$2av_{m+1} - v_m$ with initial values $v_0 = 1$ and $v_1 = a$. We show that the only possible solutions of our problem occur with $m = 1$ or 2.

It is easily seen that we cannot have $4 \mid m$. For if $m = 4k$ then $v_{4k} = 8v_k^4 - 8v_k^2 + 1$, and as is shown in [4] the equation $x^2 = 8y^4 - 8y^2 + 1$ can only be satisfied with $x = 1$, which does not give a solution to our problem.

For n odd, let $w_n = v_n/a$, which is also an integer. Then $w_{n+4} + w_{n+2} = 2v_{n+3}$ and $w_{n+2} + w_n = 2v_{n+1}$. Thus

$$w_{n+4} + 2w_{n+2} + w_n = 2(v_{n+3} + v_{n+1}) = 4av_{n+2} \equiv 0 \pmod{4a},$$

and so since $w_1 = 1$ and $w_3 \equiv -3 \pmod{4a}$, it follows that for all odd n,

$$w_n \equiv (-)^{(n-1)/2} n \pmod{4a} \tag{1}$$

and

$$w_n \equiv 1 \pmod 4. \tag{2}$$

In particular, solutions are possible for m odd only if $a = 2^{2\alpha} a_1$ where $\alpha \geq 0$ and a_1 is odd, and then if $(a, n) = 1$

$$(w_n \mid a_1) = ((-)^{(n-1)/2} n \mid a_1) = (a_1 \mid n) = (a \mid n). \tag{3}$$

Next we prove by induction on nN that for all odd coprime integers n and N the Legendre–Jacobi symbol $(w_n \mid w_N) = +1$. This holds if $nN = 1$; suppose it is true for all values less than the one we consider. $n = N$ is impossible unless $n = N = 1$ since n and N were supposed coprime; without loss of generality we may assume $n > N$, since by (2) quadratic reciprocity gives $(w_n|w_N) = (w_N|w_n)$. Then it is easily found that $w_n \equiv -w_{n-2N} \pmod{w_N}$, and again $n-2N$ and N are coprime. If here $n-2N$ is positive the induction is completed with the aid of (2); on the other hand, if $n-2N$ is negative then we use $w_{n-2N} = -w_{2N-n}$ and (2) to complete the induction, since if $N < n < 2N$, then $0 < 2N - n < N$.

Suppose first that m is odd. Ljunggren showed that there was at most one solution in this case, and we show that if it occurs it must occur for $m = 1$. For suppose that we have a solution with $m > 1$. Let n denote any odd integer coprime to am. Then

$$1 = (w_m \mid w_n) = (a \mid w_n) = (2^{2\alpha} a_1 \mid w_n) = (w_n \mid a_1) = (a \mid n),$$

by (2) and (3), and this implies that a must be a perfect square, since otherwise, we may choose n to be congruent to 1 modulo 4 and also a quadratic non-residue modulo a. But $a = v_1$ and this would contradict Ljunggren's result.

The proof for the case $m \equiv 2 \pmod 4$ follows in exactly the same way working with $\alpha^2 = A + B\sqrt{D}$ instead of α.

Combining this result with the result of [6] or [8] that the equation $y^2 = 2x^4 - 1$ has only the solutions in positive integers given by $x = 1$

and 13, we see that for both $m = 1$ and $m = 2$ to be solutions we should have $x_1^2 = a$ and $x_2^2 = 2a^2 - 1$, and then $x_2^2 = 2x_1^4 - 1$ whence $a = 1$ or 13^2; $a = 1$ gives no solution and $a = 13^2$ gives $Db^2 = 1785 \cdot 4^2$, i.e. only $D = 1785$.

Table 1 gives all solutions for D squarefree and under 150000:

Table 1

D	x	D	x	D	x	D	x	D	x
5	3	915	11	10421	35	28230	97	68295	28
6	7	985	577	12155	21	29039	143	69729	65
15	2	1111	10	13015	37	33215	27	72041	243
29	99	1295	6	13271	24	36411	107	76245	47
39	5	1785	13&239	14430	31	38415	14	108335	48
145	17	2031	26	16913	51	41943	32	112910	127
210	41	3603	49	17490	23	44205	29	127551	50
255	4	3815	251	18530	33	54795	53	129610	161
410	9	4199	18	20735	12	60639	1393	142071	70
455	8	7215	38	22327	82	61535	63	144590	39
791	15	8547	43	24414	25	63546	55		
905	19	8555	117	26390	57	65535	16		

References

[1] J. H. E. Cohn, *Eight Diophantine equations*, Proc. London Math. Soc. (3) 16 (1966), 153–166.

[2] —, *Eight Diophantine equations, addendum*, ibid. 17 (1967), 381.

[3] —, *Five Diophantine equations*, Math. Scand. 21 (1967), 61–70.

[4] —, *The Diophantine equation $x^4 - Dy^2 = 1$*, Quart. J. Math. Oxford (2) 26 (1975), 279–281.

[5] M. H. Le, *On the diophantine equation $D_1x^4 - D_2y^2 = 1$*, Acta Arith. 76 (1996), 1–9.

[6] W. Ljunggren, *Zur Theorie der Gleichung $X^2+1 = DY^4$*, Avh. Norske Vid. Akad. Oslo I. Mat.-Naturv. 1942 (5), 27 pp.

[7] —, *Über die Gleichung $x^4 - Dy^2 = 1$*, Arch. Math. Naturv. 45 (5) (1942), 61–70.

[8] R. Steiner and N. Tzanakis, *Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$*, J. Number Theory 37 (1991), 123–132.

Department of Mathematics
Royal Holloway University of London
Egham, Surrey TW20 0EX, England
E-mail: J.Cohn@rhbnc.ac.uk

Received on 24.5.1996 (2993)