ACTA ARITHMETICA
106.1 (2003)

The Diophantine equation $x^n = Dy^2 + 1$

by

J. H. E. Cohn (London)

1. Introduction. In [4] the complete set of positive integer solutions to the equation of the title is described in the case $n = 4$, which clearly includes all n divisible by 4. If $4 \nmid n$ then any $n \geq 3$ must have an odd prime factor p, and so it suffices to consider only $n = p$, an odd prime, which we shall do except in the final statement of results without further mention.

Nagell [7, Theorem 25] has proved

THEOREM 1. *Let $D = c^2 d$ with d squarefree. Then the equation of the title has no solution with x odd except perhaps if n is a factor of the class number h of the quadratic field $\mathbb{Q}[\sqrt{-d}\,]$, the sole exceptions being the solution $x = 3$, $p = 5$ when $D = 2$ or 242.*

For any given D, h is easily calculated, and is less than D, which reduces the problem to a small finite set of values of n, all of which are themselves small. In Section 2 we prove an entirely different result which achieves this for x even too.

It has also been shown in [2] that, without reference to the parity of x, for $p = 3$ there can be no solution unless D possesses a prime factor $\equiv 1 \pmod{p}$. One of the consequences of the result in Section 2 is that for x even this remains true for all p. In Section 3 we show that it also holds for x odd when $p = 5$ except if $D = 2$.

Finally, we attempt to deal with the cases $D \leq 100$.

Incidentally, Nagell's result has the following rather striking

COROLLARY 1. *Given positive integers a, and odd n, let $c^2 d = (2a+1)^n - 1$ with d squarefree. Then the class number of the quadratic field $\mathbb{Q}[\sqrt{-d}\,]$ is divisible by n except if $a = 1$ and $n = 5$.*

2. Even values of x. Nagell's method employed the factorisation of the equation of the title in the quadratic field $\mathbb{Q}[\sqrt{-d}\,]$, to obtain $x^p =$

2000 *Mathematics Subject Classification*: Primary 11D61; Secondary 11B37.
Key words and phrases: exponential Diophantine equation.

$(1+cy\sqrt{-d})(1-cy\sqrt{-d})$ where the principal ideals $[1+yc\sqrt{-d}]$ and $[1-yc\sqrt{-d}]$ are coprime and hence $[1+yc\sqrt{-d}]=\pi^p$ for some ideal π in the field. Then π^h is a principal ideal, and if $p\nmid h$, $[1+yc\sqrt{-d}]^h=(\pi^h)^p$ leads to $1+yc\sqrt{-d}=\varepsilon\alpha^p$ for some unit ε and element α of the field, from which he deduces his result. This applies only when x is odd, and when x is even, which of course could occur only if $D\equiv 7 \pmod 8$, this is no longer the case, and we should obtain instead

$$2^{p-2}\left(\frac{1}{2}x\right)^p=\left(\frac{1+cy\sqrt{-d}}{2}\right)\left(\frac{1-cy\sqrt{-d}}{2}\right) \tag{2.1}$$

which appears quite intractable without a knowledge of p. We prove

THEOREM 2.1. *There can be a solution to the equation* $x^p=Dy^2+1$ *with* x *even only if* D *has at least one prime factor* $\equiv 1 \pmod p$.

This is proved for the case $p=3$ in [2] and follows for larger p from

THEOREM 2.2. *Let* $p>3$. *Then there can be a solution to the equation* $x^p=Dy^2+1$ *with* x *even only if* $D=D_1D_2$, $D_2>1$, *every prime factor of* D_2 *is congruent to* 1 *modulo* p *and either* $x-1=D_1a^2$, $(x^p-1)/(x-1)=D_2b^2$ *or* $x-1=pD_1a^2$, $(x^p-1)/(x-1)=pD_2b^2$.

Denoting the Jacobi symbol by $(r|s)$, we prove

LEMMA 2.1. *For each positive integer* $x\equiv 0 \pmod 4$ *and each pair of relatively prime positive integers* r *and* s, $\left(\frac{x^r-1}{x-1}\middle|\frac{x^s-1}{x-1}\right)=1$.

Proof. We use induction on the quantity $r+s$, the result being trivial if $r+s=2$. Let $r+s=k$, and suppose that it holds for all values of $r+s<k$. For all n, $(x^n-1)/(x-1)\equiv 1 \pmod 4$ and so there is no loss of generality in assuming that $r>s$, and then the result follows from the identity $x^r-1=x^{r-s}(x^s-1)+(x^{r-s}-1)$ yielding

$$\left(\frac{x^r-1}{x-1}\middle|\frac{x^s-1}{x-1}\right)=\left(\frac{x^{r-s}-1}{x-1}\middle|\frac{x^s-1}{x-1}\right).$$

LEMMA 2.2. *Let* $p>3$ *denote a prime. Then there are no solutions with* x *even to the equation* $(x^p-1)/(x-1)=py^2$.

Proof. For any solution $x\equiv 1 \pmod p$ since otherwise $(x^p-1)/(x-1)\equiv 1 \pmod p$.

If $p\equiv 1 \pmod 4$, then for x even, $py^2=x^{p-1}+x^{p-2}+\ldots+x+1$ implies that $4\mid x$. Suppose that $x=1+\lambda p^r$ where $p\nmid\lambda$. Then if $(p,q)=1$ we obtain, using the previous lemma,

$$1=\left(\frac{x^p-1}{x-1}\middle|\frac{x^q-1}{x-1}\right)=\left(py^2\middle|\frac{x^q-1}{x-1}\right)=\left(p\middle|\frac{x^q-1}{x-1}\right)=\left(\frac{x^q-1}{x-1}\middle|p\right).$$

However,

$$\frac{x^q - 1}{x - 1} = \frac{(\lambda p^r + 1)^q - 1}{\lambda p^r} \equiv q \pmod{p},$$

and this yields a contradiction on taking q to be a quadratic non-residue modulo p.

If $p \equiv 3 \pmod{4}$, then $py^2 = x^{p-1} + x^{p-2} + \ldots + x + 1$ with x even implies that $2 \,\|\, x$. Thus there is no solution if $p \equiv 7 \pmod{8}$, for then $py^2 \equiv 1 \pmod{(x+1)}$, but $(p|x+1) = -(x+1|p) = -(2|p) = -1$ since $x \equiv 1 \pmod{p}$.

Finally, if $p \equiv 3 \pmod{8}$, then $x \equiv 6 \pmod{8}$, and so for any $a \geq 3$, $(x^a - 1)/(x-1) \equiv 3 \pmod{8}$, whence

$$\left(x \,\middle|\, \frac{x^a - 1}{x - 1}\right) = -\left(\frac{x}{2} \,\middle|\, \frac{x^a - 1}{x - 1}\right) = \left(\frac{x^a - 1}{x - 1} \,\middle|\, \frac{x}{2}\right) = 1.$$

But, since $x^p - 1 = (x^{(p-1)/2} - 1) + (x^{(p+1)/2} - 1)x^{(p-1)/2}$, we also have as $p > 3$,

$$\begin{aligned}
\left(\frac{x^p - 1}{x - 1} \,\middle|\, \frac{x^{(p+1)/2} - 1}{x - 1}\right) &= \left(\frac{x^{(p-1)/2} - 1}{x - 1} \,\middle|\, \frac{x^{(p+1)/2} - 1}{x - 1}\right) \\
&= -\left(\frac{x^{(p+1)/2} - 1}{x - 1} \,\middle|\, \frac{x^{(p-1)/2} - 1}{x - 1}\right) \\
&= -\left(\frac{x^{(p+1)/2} - x^{(p-1)/2}}{x - 1} \,\middle|\, \frac{x^{(p-1)/2} - 1}{x - 1}\right) \\
&= -\left(x \,\middle|\, \frac{x^{(p-1)/2} - 1}{x - 1}\right)^{(p-1)/2} = -1,
\end{aligned}$$

and so $(x^p - 1)/(x - 1) = py^2$ gives

$$\left(p \,\middle|\, \frac{x^{(p+1)/2} - 1}{x - 1}\right) = -1 \quad \text{whence} \quad \left(\frac{x^{(p+1)/2} - 1}{x - 1} \,\middle|\, p\right) = 1.$$

But, as before, $(x^{(p+1)/2} - 1)/(x - 1) \equiv (p+1)/2 \pmod{p}$ in view of $x \equiv 1 \pmod{p}$, and then this is impossible since $p \equiv 3 \pmod{8}$. This concludes the proof of the lemma.

LEMMA 2.3. *The only solutions of the equation $(x^n - 1)/(x - 1) = y^2$ in positive integers $x > 1$, y and $n > 2$ are $n = 4$, $x = 7$, $y = 20$ and $n = 5$, $x = 3$, $y = 11$.*

This result is Sats 1 in [6]. For future reference we note the following

COROLLARY 2. *The equation $d^2 = x^4 + x^3 + x^2 + x + 1$ has only the solution $x = 3$, $d = 11$ in positive integers.*

Proof of Theorem 2.2. From the equation we obtain

$$Dy^2 = (x-1)\left(\frac{x^p-1}{x-1}\right);$$

it is easily shown that the factors on the right are coprime or have common factor p precisely, and that the second is not divisible by p^2. Thus we must have *either* $x-1 = D_1a^2$, $(x^p-1)/(x-1) = D_2b^2$ *or* $x-1 = pD_1a^2$, $(x^p-1)/(x-1) = pD_2b^2$ where $D = D_1D_2$ and $p \nmid D_2$. Here we cannot have $D_2 = 1$ for x even in the first case by Lemma 2.3, nor in the second by Lemma 2.2. Thus $D_2 > 1$.

If a prime q divides D_2, then certainly it is odd and does not divide $x-1$, so that $x^p \equiv 1 \pmod q$ and $x^{q-1} \equiv 1 \pmod q$ imply that $x^{(p,q-1)} \equiv 1 \pmod q$ and this is possible only if $p \mid (q-1)$, i.e. $q \equiv 1 \pmod p$.

This concludes the proof.

Nagell's result showed that for a given D, in considering the equation of the title for odd values of x, we could restrict our attention to the finite set of prime indices dividing the class number, h; the consequence of Theorem 2.1 is that for even values of x we also need consider only a finite set of prime indices, in this case those dividing $q-1$ for primes q dividing D. This provides help with the solution of (2.1), and in view of the theorem of Siegel that for any given $n > 2$ there can be only finitely many solutions yields a simple proof of

THEOREM 2.3. *For given D, the equation of the title has only finitely many solutions in positive integers x, y and $n \geq 3$.*

This is a special case of a deep analytical result; see e.g. [8, Theorem 12.2].

We quote for future reference another result of Ljunggren's, Satz XVIII in [5].

LEMMA 2.4. *For any D, the equation $x^2 = Dy^4 + 1$ has at most two solutions in positive integers x and y.*

3. The case $p = 5$. We extend the result of [2] to the case $p = 5$, without restricting x to be even.

THEOREM 3.1. *The equation $x^5 = 2y^2 + 1$ has the single solution $x = 3$. If $D > 2$ and D has no prime factor $\equiv 1 \pmod 5$, then the equation $x^5 = Dy^2 + 1$ has no solution in positive integers.*

LEMMA 3.1. *The equation $z^2 = x^4 + 50x^2y^2 + 125y^4$ has no solutions in integers with $y \neq 0$.*

Proof. Suppose on the contrary that there were solutions in positive integers and that of all such solutions, x, y, z was one with y minimal. Then

x, $5y$ and z must be pairwise coprime, and so $z^2 = (x^2 + 25y^2)^2 - 500y^4$ gives

$$125y^4 = \left(\tfrac{1}{2}(x^2 + 25y^2 + z)\right)\left(\tfrac{1}{2}(x^2 + 25y^2 - z)\right),$$

where the two factors on the right must be coprime since any common prime factor q would have to divide both $5y$ and z. Thus for some integers a and b with $(a, 5b) = 1$ we should obtain

$$x^2 + 25y^2 \pm z = 2a^4, \qquad x^2 + 25y^2 \mp z = 250b^4, \qquad y = ab,$$

and then

$$x^2 = a^4 - 25a^2b^2 + 125b^4.$$

Here a and b cannot both be even, since $(a, 5b) = 1$, and cannot both be odd, else $x^2 \equiv 5 \pmod 8$. Thus a and b have opposite parity and x is odd and since $x^2 + b^4 = (a^2 - 7b^2)(a^2 - 18b^2)$, the factors on the right are of the same sign. If a is even, the first factor must be positive, otherwise the Jacobi symbol $(-1|7b^2 - a^2) = -1$, and if a is odd the second one must be positive else $(-1|18b^2 - a^2) = -1$. Thus in either case $a^2 > 18b^2$.

Then

$$x^2 = \left(a^2 - \frac{25}{2}b^2\right)^2 - \frac{125}{4}b^4$$

and now if $b = 2c$ is even, then

$$125c^4 = \left(\tfrac{1}{2}(a^2 - 50c^2 + x)\right)\left(\tfrac{1}{2}(a^2 - 50c^2 - x)\right)$$

with both factors on the right positive and again coprime, whence $c = de$, $a^2 - 50c^2 \pm x = 2d^4$ and $a^2 - 50c^2 \mp x = 250e^4$, and then $a^2 = d^4 + 50d^2e^2 + 125e^4$, completing the descent since $y = ab = 2ade > e$. On the other hand, if b is odd we obtain similarly

$$125b^4 = (2a^2 - 25b^2 + 2x)(2a^2 - 25b^2 - 2x)$$

and then $b = de$, $2a^2 - 25b^2 \pm 2x = d^4$ and $2a^2 - 25b^2 \mp 2x = 125e^4$, yielding $(2a)^2 = d^4 + 50d^2e^2 + 125e^4$, and again the descent is complete since now $y = ab = ade > e$ unless $a = d = 1$, which gives no solution. This concludes the proof of the lemma.

COROLLARY 3. *The equation $5z^2 = x^4 + x^3y + x^2y^2 + xy^3 + y^4$ has no solutions in integers other than $x = y$.*

Proof. For a solution, let $\xi = x + y$, $\eta = x - y$. Then $80z^2 = 5\xi^4 + 10\xi^2\eta^2 + \eta^4$, and so with $\eta = 5\zeta$ we obtain $(4z)^2 = \xi^4 + 50\xi^2\zeta^2 + 125\zeta^4$.

Proof of Theorem 3.1. From the equation, we obtain

$$Dy^2 = (x - 1)(x^4 + x^3 + x^2 + x + 1),$$

where the factors on the right have common factor 1 or 5. Now it is impossible that an odd power of a prime q other than 5 divides the second factor, for if so we should find that $q \mid D$, $x \not\equiv 1 \pmod q$ and $x^5 \equiv 1 \pmod q$. But then we should find that $5 \mid (q-1)$, and the hypothesis of the theorem is that D has no such prime factor. Thus we see that we must have *either* $x^4+x^3+x^2+x+1 = z^2$ *or* $5z^2$. By Corollary 2, the first implies that $x=3$, giving just $D=2$, and by the corollary to Lemma 3.1, the second implies $x=1$, which does not give a solution with y positive.

Although we shall make no use of the fact and omit the proof, we may show in the same way

Theorem 3.2. *The equation $x^5 = 2y^2-1$ has the single solution $x=1$. If $D>2$ and D has no prime factor $\equiv 1 \pmod 5$, then the equation $x^5 = Dy^2-1$ has no solution in positive integers.*

4. Small values of D. In this section we apply results from previous sections in an attempt to describe the complete set of positive integer solutions to the equation of the title for all cases with $D \le 100$. At the outset, we observe that it is enough to consider the cases with D squarefree. By [4] there are solutions with $4 \mid n$ for precisely five values of D given by $(D,x,y,n) = (5,3,4,4)$, $(6,7,20,4)$, $(15,2,1,4)$, $(29,99,1820,4)$ and $(39,5,4,4)$. There are also eleven values with $D \equiv 7 \pmod 8$ for which we have to consider even x, and by Nagell's result, there is the single solution $p=5$, $x=3$ when $D=2$, and 17 cases in which an odd prime divides the corresponding class number. These may be categorised as follows:

(a) four cases with $p=3$ for which there are known solutions, $D = 26, 31, 38$ and 61;
(b) eight other cases with $p=3$, $D = 23, 29, 53, 59, 83, 87, 89$ and 92;
(c) four cases with $p=5$, $D = 47, 74, 79$ and 86;
(d) one case, $D=71$, with $p=7$.

There are no solutions, odd or even, in the eight cases of (b) by the result of [2], nor in the four cases of (c) by Theorem 3.1. We now consider some of the remaining equations.

Result 4.1. *The only solutions in positive integers of $x^3 = 26y^2+1$ are $y=1$ and 1086.*

Proof. We obtain $(x-1)(x^2+x+1) = 26y^2$ where the factors on the left have common factor 1 or 3 and the second is odd; there are therefore four cases to consider.

Case 1: $x-1 = 26a^2$, $x^2+x+1 = b^2$ *with* $y = ab$. Here the second is impossible as can be seen on completing the square.

Case 2: $x-1 = 6a^2$, $x^2+x+1 = 39b^2$ *with* $y = 3ab$. Here the former implies that $x \equiv 1$ or $-1 \pmod 8$, both of which are inconsistent with the latter.

Case 3: $x-1 = 78a^2$, $x^2+x+1 = 3b^2$ *with* $y = 3ab$. Here the second leads to $(2b)^2 - 3\left(\frac{2x+1}{3}\right)^2 = 1$, and so

$$\frac{2x+1}{3} = \frac{(2+\sqrt{3})^k - (2-\sqrt{3})^k}{2\sqrt{3}} = u_k,$$

say. Let $v_k = ((2+\sqrt{3})^k + (2-\sqrt{3})^k)/2$. Then we find that $52a^2 = u_k - 1$, and it is easily verified that $u_k \equiv 1 \pmod 4$ implies that $k \equiv 1 \pmod 4$ and then with $k = 4m+1$ we find that $52a^2 = u_{4m+1} - u_1 = 2v_{2m+1}u_{2m}$ and so $13\left(\frac{1}{2}a\right)^2 = \left(\frac{1}{2}v_{2m+1}\right)\left(\frac{1}{4}u_{2m}\right)$ where the factors on the right are coprime. Thus we see that *either* $v_{2m+1} = 2\lambda^2$ *or* $u_{2m} = \lambda^2$. The former then gives $4\lambda^4 - 3u_{2m+1}^2 = 1$, which holds only for $\lambda = 1$ as is shown in [2, Lemma 2], and then $k = 1$ whence $a = 0$ and so no solution in positive integers arises. The latter yields $v_{2m}^2 = 3\lambda^4 + 1$, which holds only for $\lambda = 0, 1$ or 2 by Lemma 2.4. Here $\lambda = 0$ leads to $y = 0$ again, $\lambda = 1$ gives no solution since u_{2m} is even, and $\lambda = 2$ gives $k = 5$, and then $a = 2$, and $x = 313$, $y = 1086$.

Case 4: $x-1 = 2a^2$, $x^2+x+1 = 13b^2$ *with* $y = ab$. Clearly one solution is $x = 3$, $y = 1$; the difficulty is to show that there are no more. We find that $(2x+1)^2 - 52b^2 = -3$, and so $2x+1+2b\sqrt{13} = (\pm 7 + 2\sqrt{13})(649 + 180\sqrt{13})^k$. Thus $2x+1 \equiv \pm 1 \pmod 3$ and the lower sign is impossible since it is incompatible with $x - 1 = 2a^2$. Thus

$$2x+1+2b\sqrt{13} = (7+2\sqrt{13})(649+180\sqrt{13})^k, \tag{4.1}$$

and our first task is to show that k must be a multiple of 4.

We see that $649 + 180\sqrt{13} \equiv 4\sqrt{13} \pmod{11}$ and that $(649+180\sqrt{13})^2 \equiv -1 \pmod{11}$ and so $k \equiv 1 \pmod 4$ is impossible since it would give $2x+1 \equiv 5 \pmod{11}$, inconsistent with $x - 1 = 2a^2$. Similarly $649 + 180\sqrt{13} \equiv 3\sqrt{13}$ and $(649+180\sqrt{13})^2 \equiv -1 \pmod{59}$, and so $k \equiv 3 \pmod 4$ would give $2x+1 \equiv -19 \pmod{59}$, whence $2a^2 \equiv -11 \pmod{59}$, impossible since $(2|59) = -1$, whereas $(-11|59) = +1$. So k must be even, say $k = 2l$. We then find that

$$2x+1+2b\sqrt{13} = (7+2\sqrt{13})(842401 + 233640\sqrt{13})^l,$$

and arguing similarly modulo 7 we find that $l \equiv 3 \pmod 4$ is impossible, and modulo 17 that $l \not\equiv 1 \pmod 4$. Thus k must be a multiple of 4, say $k = 4m$. Then (4.1) gives

$$\begin{aligned} 2x+1+2b\sqrt{13} &= (7+2\sqrt{13})(649+180\sqrt{13})^{4m} \\ &= (7+2\sqrt{13})\left(\frac{3+\sqrt{13}}{2}\right)^{24m} = (7+2\sqrt{13})\alpha^{24m}, \end{aligned}$$

say, and so $4x + 2 = 7Q_{24m} + 26P_{24m}$ where β is the conjugate of α and the sequences $\{P_n\}$ and $\{Q_n\}$ are defined by $P_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ and

$Q_n = \alpha^n + \beta^n$, as in [1, with $x = 3$], and both satisfy the recurrence relation $w_{n+2} = 3w_{n+1} + w_n$ with initial values $P_0 = 0$, $P_1 = 1$, $Q_0 = 2$, $Q_1 = 3$. Thus we should require $8a^2 = 7Q_{24m} + 26P_{24m} - 6$, and here $m = 0$ gives the solution $a = 1$. However for $m \neq 0$, we may write $24m = 2\lambda t$ where λ is odd and $t = 2^r$ with $r \geq 2$. Now as in [1], we find that $Q_{n+2t} \equiv -Q_n \pmod{Q_t}$ and $P_{n+2t} \equiv -P_n \pmod{Q_t}$ and so $8a^2 \equiv -7Q_0 - 26P_0 - 6 = -20 \pmod{Q_t}$. But since $Q_{2s} = Q_s^2 - 2$ for any even s, in view of $Q_4 = 119 \equiv -1 \pmod{40}$ it follows by induction on r that $Q_t \equiv -1 \pmod{40}$ for all $t = 2^r$ with $r \geq 2$. Thus $2a^2 \equiv -5 \pmod{Q_t}$ is impossible since $(2|Q_t) = +1$ whereas $(-5|Q_t) = -1$. This concludes the proof.

Result 4.2. *The only solutions of the equation $x^n = 7y^2 + 1$ in positive integers x, y and $n \geq 3$ are given by $y = 1$ and $y = 3$.*

It is shown in [9] that there are no solutions apart from those stated if $3 \mid n$, in [4] that there are none for $4 \mid n$, and by Theorem 1 that there are none for any odd x. The conclusion therefore follows from Theorem 2.1.

Result 4.3. *The only solution of the equation $x^n = 15y^2 + 1$ in positive integers x, y and $n \geq 3$ is given by $y = 1$.*

By [4] the only solution with $4 \mid n$ is given by $y = 1$. If n is an odd prime, then there is no solution for $n = 3$ by [2], none with x odd by Theorem 1, nor for x even by Theorem 2.1.

Result 4.4. *The equation $x^n = 23y^2 + 1$ has no solution in positive integers x, y and $n \geq 3$.*

Here, there are no solutions with $4 \mid n$ by [4], none for $n = 3$ by [2] and none for other odd values of n and x by Theorem 1. By Theorem 2.2, the only remaining possibilities for x even are

$$\textit{either} \quad x - 1 = a^2, \ \frac{x^{11} - 1}{x - 1} = 23b^2 \quad \textit{or} \quad x - 1 = 11a^2, \ \frac{x^{11} - 1}{x - 1} = 23 \cdot 11b^2.$$

In the first case, the first equation would imply $x \equiv 2 \pmod 8$ and $(x - 1|23) = 1$, and the second equation $23b^2 \equiv 1 \pmod x$, yielding $(x|23) = \left(\frac{x}{2}|23\right) = \left(23|\frac{x}{2}\right) = 1$, and similarly $(x + 1|23) = -1$ and $(x^2 + x + 1|23) = 1$. It is now easily verified that no x satisfies $(x|23) = 1$, $(x - 1|23) = 1$, $(x + 1|23) = -1$, and $(x^2 + x + 1|23) = 1$, and so this case does not arise.

In the second case $(x - 1|23) = -1$ and since $23|(x^{11} - 1)$, x is a quadratic residue modulo 23, i.e., $(x|23) = 1$. Also since $x - 1 = 11a^2$, $x \equiv 0 \pmod 4$ and then for any odd q not divisible by 11, Lemma 2.1 yields $\left(11 \cdot 23\middle|\frac{x^q - 1}{x - 1}\right)$ $= 1$ whence

$$\left(\frac{x^q - 1}{x - 1}\middle|23\right) = \left(\frac{x^q - 1}{x - 1}\middle|11\right) = \left(\frac{(1 + 11a^2)^q - 1}{11a^2}\middle|11\right) = (q|11).$$

Putting $q = 3$ in this gives $(x^2 + x + 1|23) = 1$, and this together with $(x - 1|23) = -1$ and $(x|23) = 1$ implies $x \equiv 8 \pmod{23}$. But now $q = 7$ gives $(x^6 + x^5 + \ldots + 1|23) = -1$ and $x \equiv 8 \pmod{23}$ does not satisfy this, concluding the proof.

We have settled all but six of the cases with $D \leq 100$ in similar fashion, and a summary of results follows. I have a set of notes outlining the proofs of the various cases which I am willing to send to any interested reader.

5. Statement of results for $D \leq 100$. There are the following solutions:

D	y	x	n	D	y	x	n	D	y	x	n
2	11	3	5	20	2	3	4	38	3	7	3
5	4	3	4	24	10	7	4	39	4	5	4
6	20	7	4	26	1	3	3	61	6	13	3
7	1	2	3	26	1086	313	3	63	1	2	6
7	3	2	6	29	1820	99	4	63	1	4	3
7	3	4	3	31	1	2	5	80	1	3	4
15	1	2	4	31	2	5	3	96	5	7	4

The following cases remain open, although it is conjectured that there are no solutions other than the known ones:

D	p	Status
31	3	apart from the known solution $x = 5$ maybe more with x odd
31	5	apart from the known solution $x = 2$ maybe more with x even
38	3	apart from the known solution $x = 7$ maybe more with x odd
61	3	apart from the known solution $x = 13$ maybe more with x odd
71	5	even values of x open
71	7	odd values of x open

There are no solutions at all for any of the remaining values of D.

6. Perfect powers in the associated Pell sequence. The above methods also provide a solution to another problem. The Pell sequence $\{P_n\}$ and its associated sequence $\{Q_n\}$ are defined by the recurrence relation $w_{n+2} = 2w_{n+1} + w_n$ with initial values $P_0 = 0$, $P_1 = 1$, $Q_0 = Q_1 = 1$. They generate the general solution of the Pell equation $Q^2 - 2P^2 = \pm 1$. It is known [3] that the only perfect powers in the former are 0, 1 and 169. We can now prove

THEOREM 6.1. *The only perfect power in the associated Pell sequence is* 1.

Lemma 6.1. *Let* $x \equiv 0$ *or* $1 \pmod 4$. *Then* $\left(\frac{x^r+1}{x+1}\middle|\frac{x^s+1}{x+1}\right) = 1$ *for all relatively prime odd integers* r *and* s.

The proof is exactly similar to that of Lemma 2.1 and is omitted.

Proof of Theorem 6.1. Suppose that $Q = x^p$ where p denote a prime. No solution apart from $Q = 1$ arises with $p = 2$ since then $P^4 \pm x^4 = (P^2 \pm 1)^2$. For p odd, our equation is $x^{2p} = 2y^2 \pm 1$, and with the upper sign there are no solutions by Theorem 1. The lower sign gives

$$y^2 = \left(\frac{x^2+1}{2}\right)(x^{2p-2} - x^{2p-4} + \ldots - x^2 + 1),$$

where the factors on the right have common factor 1 or p. The former would give

$$b^2 = x^{2p-2} - x^{2p-4} + \ldots - x^2 + 1 = \frac{x^{2p}+1}{x^2+1},$$

and this has no solution with $x > 1$ by [6]. The latter gives $x^2 + 1 = 2pa^2$,

$$pb^2 = x^{2p-2} - x^{2p-4} + \ldots - x^2 + 1 = \frac{x^{2p}+1}{x^2+1}$$

with $x^2 \equiv 1 \pmod 8$, and $p \equiv 1 \pmod 8$. But then for any odd integer r coprime to p we should find that

$$\left(pb^2\middle|\frac{x^{2r}+1}{x^2+1}\right) = \left(\frac{x^{2p}+1}{x^2+1}\middle|\frac{x^{2r}+1}{x^2+1}\right) = 1$$

by Lemma 6.1, and so $\left(\frac{x^{2r}+1}{x^2+1}\middle|p\right) = 1$. But

$$\frac{x^{2r}+1}{x^2+1} = \frac{(2pa^2-1)^r+1}{2pa^2} \equiv r \pmod p,$$

and so we have a contradiction on selecting r to be an odd quadratic non-residue modulo p, concluding the proof.

Added in proof. The author wishes to thank Professor Schinzel for pointing out that Lemmas 2.1 and 6.1 are particular cases of the more general results contained in Theorem $2'$, $5''$ and $6'$ of the paper by A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.

References

[1] J. H. E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. 41 (1972), 631–646.

[2] —, *The Diophantine equations* $x^3 = Ny^2 \pm 1$, Quart. J. Math. Oxford (2) 42 (1991), 27–30.

[3] —, *Perfect Pell powers*, Glasgow Math. J. 38 (1996), 19–20.

[4] —, *The Diophantine equation* $x^4 - Dy^2 = 1$, *II*, Acta Arith. 78 (1997), 401–403.

[5] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer usw.*, Oslo Vid. Akad. Skrifter 1936, nr 12.

[6] —, *Noen setninger om ubestemte likninger av formen* $\frac{x^n-1}{x-1} = y^q$, Norsk Matematisk Tidsskrift 25 (1943), 17–20.

[7] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Regiae Soc. Sci. Uppsal. (4) 16 (1955), 1–38.

[8] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, Cambridge, 1986.

[9] R. J. Stroeker, *On the Diophantine equation* $x^3 - Dy^2 = 1$, Nieuw. Arch. Wisk. (3) 24 (1976), 231–255.

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

Received on 26.7.2001
and in revised form on 23.1.2002 (4028)