MATH. SCAND. 18 (1966), 69–86

ON THE DIOPHANTINE EQUATION $Cx^2+D = 2y^n$

W. LJUNGGREN

Dedicated to professor T. Nagell on his 70th birthday

Introduction.

Let Q denote the field of rational numbers and let further integers in Q be denoted by Roman letters denote. The diophantine equation

$$(1) \qquad ax^2+bx+c = dy^n ,$$

where a, b, c and d are integers, $a \neq 0$, $b^2-4ac \neq 0$, $d \neq 0$, has only a finite number of solutions in integers x and y when $n \geqq 3$. This was first shown by A. Thue and later on by Landau and Ostrowski. See for instance [15]. However, no general method is known for determining all integral solutions x and y for a given equation of the form (1).

In this paper we confine ourselves to the study of such equations of the form (1) where it is possible to derive criteria for solubility which are valid for comprehensive classes of odd exponents n.

A complete solution of the equation $x^2+1=y^{2m+1}$ was already given by V. A. Lebesgue [3] in 1850. In 1895 C. Störmer showed that the equation $x^2+1=2y^{2m+1}$ has no solutions with $y>1$. The first more general results of the type mentioned above, were obtained by T. Nagell in papers from 1921 [12] and 1923 [14]. As an example we quote the following theorem: Let D denote a positive integer without any squared factor >1. Assume that the number of classes of ideals of $Q((-D)^{\frac{1}{2}})$ is not divisible by the odd positive integer n. Then the diophantine equation

$$(2) \qquad 1+Dx^2 = y^n$$

has no solutions in integers x and y if $y>1$ and odd, with the exception of the solution $1+2\cdot 11^2=3^5$.

It is well known that the solution of (1) can be brought back to the solution in rational integers of a finite number of equations of the form $f(u,v)=g$, where $f(u,v)$ is a binary form of degree n with integral coefficients and g an integer taken from a finite set. Under the given conditions concerning the equation (2) the binary forms in question are reducible, giving only a finite number of possibilities for u or v. The proof is accomplished by means of congruence considerations.

Received May 22, 1965.

Nagell has continued his investigations in a series of papers [16]–[19]. Other contributions to the theory are due to W. Ljunggren [5]–[11], B. Stolt [22], [23], B. Persson [21] and D. J. Lewis [4].

Let C and D, $D>1$, denote odd positive integers, $CD\equiv 1 \pmod 4$ and CD without any squared factor >1. Let further h denote the number of classes of ideals in $Q((-CD)^{\frac{1}{2}})$, and suppose $h \not\equiv 0 \pmod n$. In this paper we shall prove the following three theorems concerning the diophantine equation

$$Cx^2+D = 2y^n\,. \tag{3}$$

Theorem 1. *Let n be the power of a prime $q\equiv 1 \pmod 4$. Then the diophantine equation* (3) *has no solution in integers x,y if either*

$$D^2-1 = 2^{2m+1}D_1, \qquad (D_1,2) = 1$$

or

$$D^2-1 = 2^{2m}D_2, \qquad (D_2,2) = 1 \text{ and } q \not\equiv D_2 \pmod 8)\,.$$

Theorem 2. *Let n be the power of a prime $q\equiv \pm 3 \pmod 8$ and $C=1$ if $q\equiv 3 \pmod 8$. Then the diophantine equation* (3) *has only a finite number of solutions in natural numbers x, y and q, which can always be obtained in a finite number of steps.*

Theorem 3. *Let n be the power of a prime $q\equiv 7 \pmod 8$ and let $C=1$ Then* (3) *has no solutions in integers x, y in the following cases*:

1° $D\equiv 5 \pmod{24}$,

2° $D\equiv 13 \pmod{24}$ *and* $D+2=3^{2m+1}D'$, $(D',3)=1$,

3° $D\equiv 9$ or $21 \pmod{40}$,

4° $D\equiv 15+2\nu \pmod{40}$ *and* $D-2\nu=5^{2m+1}D'$, $(D',5)=1$, $\nu=\pm 1$.

In proving the first theorem, the formula (18) in section 2 plays an important role. In the proof of the second theorem we make use of the following lemma due to J. W. S. Cassels [1]:

Let Π be a finite set of rational primes and let P be the set of positive integers all of whose prime factors are in Π. Let $D>0$ and $E\neq 0$ be rational integers and suppose that no prime factors of E is in Π. Then there are only a finite number of solutions Z,Y of the equation

$$Z^2-DY^2 = E\,,$$

where Z is a rational integer and $Y\in P$. These can all be obtained in a finite number of steps.

1. Proof of some lemmas.

At first we show that (3), in case n is the power of any odd prime q, $CD\equiv 1 \pmod 4$ and $h\not\equiv 0 \pmod n$, implies

$$\frac{xC^{\frac{1}{2}}+(-D)^{\frac{1}{2}}}{2^{\frac{1}{2}}} = \left(\frac{aC^{\frac{1}{2}}+b(-D)^{\frac{1}{2}}}{2^{\frac{1}{2}}}\right)^q \tag{4}$$

a,b denoting odd rational integers.

The principal ideals

$$[Cx+(-CD)^{\frac{1}{2}}] \quad \text{and} \quad [Cx-(-CD)^{\frac{1}{2}}]$$

have the greatest common ideal divisor $[2C,C+(-CD)^{\frac{1}{2}}]$, because

$$[2C] = [2C,C+(-CD)^{\frac{1}{2}}]^2 \quad \text{and} \quad (x,y) = 1 .$$

From (3) it then follows that

$$[Cx+(-CD)^{\frac{1}{2}}] = [2C,C+(-CD)^{\frac{1}{2}}]\,\mathfrak{i}^{q^\alpha} ,$$

where $\mathfrak{i}$ denotes an ideal of the field $Q((-CD)^{\frac{1}{2}})$. Further we get

$$[Cx+(-CD)^{\frac{1}{2}}]^2 = [2C]\,\mathfrak{i}_1^{q^\alpha}, \qquad \mathfrak{i}_1 = \mathfrak{i}^2 . \tag{5}$$

If the class number h is divisible by q^β, $0 \leqq \beta < \alpha$, and not by $q^{\beta+1}$, there exist two rational integers f and g such that

$$fq^\alpha - gh = q^\beta .$$

Then by (5) we get the following equivalence

$$\mathfrak{i}_1^{q^\beta} \sim \mathfrak{i}_1^{fq^\alpha} \sim 1 .$$

Hence we obtain the ideal equation

$$[Cx+(-CD)^{\frac{1}{2}}]^2 = [2C][u+v(-CD)^{\frac{1}{2}}]^{q^{\alpha-\beta}} , \tag{6}$$

where u and v are rational integers. Since $CD \neq 1$, $\neq 3$, all units in the field $Q((-CD)^{\frac{1}{2}})$ are qth powers. Then it follows from (6) that

$$(Cx+(-CD)^{\frac{1}{2}})^2 = 2C(u_1+v_1(-CD)^{\frac{1}{2}})^q . \tag{7}$$

By means of (7) we derive

$$\begin{aligned} 2C(u_1+v_1(-CD)^{\frac{1}{2}}) &= (Cx+(-CD)^{\frac{1}{2}})^2(u_1+v_1(-CD)^{\frac{1}{2}})^{1-q} \\ &= (u_2+v_2(-CD)^{\frac{1}{2}})^2 . \end{aligned} \tag{8}$$

Since the last number on the right-hand side of (8) is an integer in $Q((-CD)^{\frac{1}{2}})$, u_2 and v_2 must be rational integers. It is further easy to see that $u_2 \equiv 0 \pmod{C}$, such that we can rewrite (8) in the form

$$2C(u_1+v_1(-CD)^{\frac{1}{2}}) = (Ca+b(-CD)^{\frac{1}{2}})^2 .$$

Inserting this expression in (7) we get equation (4).

Now we make use of the well-known formula [20, p. 154]:

$$(9)\qquad \frac{x^m-y^m}{x-y}=\sum_{r=0}^{\frac{1}{2}(m-1)}\frac{m}{m-r}\binom{m-r}{r}(x-y)^{m-2r-1}(xy)^r,\qquad m=1,3,5,7,\ldots .$$

Putting here

$$x=\frac{aC^{\frac{1}{2}}+b(-D)^{\frac{1}{2}}}{2^{\frac{1}{2}}},\qquad y=\frac{aC^{\frac{1}{2}}-b(-D)^{\frac{1}{2}}}{2^{\frac{1}{2}}}$$

and $m=q$ we get from (4)

$$(10)\qquad \frac{1}{b}=\frac{x^q-y^q}{x-y}=\sum_{r=0}^{\frac{1}{2}(q-1)}\frac{q}{q-r}\binom{q-r}{r}(-2Db^2)^{\frac{1}{2}(q-1)-r}\left(\frac{Ca^2+Db^2}{2}\right)^r,$$

whence $b=\pm 1$.

Mod q we find $b\equiv(-2D)^{\frac{1}{2}(q-1)}\ (\mathrm{mod}\,q)$, that is,

$$(11)\qquad b=\left(\frac{-2D}{q}\right),$$

where (10) is impossible if q divides D.

Treating (10) as a congruence mod 4, we obtain in case $q\equiv 1\ (\mathrm{mod}\,4)$

$$b\equiv q-\tfrac{1}{12}q(q^2-1)\quad(\mathrm{mod}\,4),$$

whence

$$b=(-1)^{\frac{1}{4}(q-1)}.$$

In case $q\equiv 3\ (\mathrm{mod}\,4)$ we find

$$b\equiv\tfrac{3}{2}(Ca^2+D)+\tfrac{1}{24}q(q^2-1)2\quad(\mathrm{mod}\,4),$$

or

$$(12)\qquad b\equiv-\tfrac{1}{2}(C+D)+\tfrac{1}{24}q(q^2-1)2\quad(\mathrm{mod}\,4).$$

We distinguish between two cases:

1° If $q\equiv-1\ (\mathrm{mod}\,8)$ we get from (12) that

$$b\equiv-\tfrac{1}{2}(C+D)\quad(\mathrm{mod}\,4),$$

or

$$b\equiv-D\quad(\mathrm{mod}\,4)\quad\text{if}\quad CD\equiv 1\quad(\mathrm{mod}\,8),$$

$$b\equiv D\quad(\mathrm{mod}\,4)\quad\text{if}\quad CD\equiv 5\quad(\mathrm{mod}\,8).$$

This can also be written

$$b=-(-1)^{\frac{1}{4}(q+CD)}\quad\text{if}\quad C\equiv D\equiv 1\quad(\mathrm{mod}\,4),$$

$$b=(-1)^{\frac{1}{4}(q+CD)}\quad\text{if}\quad C\equiv D\equiv -1\quad(\mathrm{mod}\,4)$$

2° If $q \equiv 3 \pmod 8$ it is easily seen that we obtain the same result as in case 1°.

Then we prove the following lemma:

LEMMA 1. *A necessary condition that the equation* (4) *be satisfied in integers x,y is that*

$$\begin{aligned} b &= (-1)^{\frac14(q-1)} && \textit{if} \quad q \equiv 1 \pmod 4 , \\ b &= -\varepsilon(-1)^{\frac14(q+CD)} && \textit{if} \quad q \equiv 3 \pmod 4 \ \textit{and} \ C \equiv D \equiv \varepsilon \pmod 4 , \end{aligned}$$

where $\varepsilon = \pm 1$.

To prove theorem 3, we have to establish some simple lemmas concerning the solubility of the equation (4).

LEMMA 2. *If the equation* (4) *is satisfied with* $q > 3$, $a \equiv 0 \pmod 3$ *and* $(C,3) = 1$, *then either*

$$q \equiv 1 \pmod 8 \quad \textit{and} \quad D^2-4 = 3^{2m_1}D_2, \ (D_2,3) = 1 ,$$

or

$$q \equiv 3 \pmod 4 \quad \textit{and} \quad D-2\varepsilon(-1)^{\frac14(q+CD)} = 3^{2m_2}D_3, \ (D_3,3) = 1 ,$$

where $C \equiv D \equiv \varepsilon \pmod 4$, $\varepsilon = \pm 1$.

If $a \equiv 0 \pmod 3$ *and* $(C,3) = 3$, *then all even exponents are to be changed into odd ones.*

PROOF. Equation (4) implies

$$D^{\frac12(q-1)} - b(-2)^{\frac12(q-1)} = \sum_{i=1}^{\frac12(q-1)} (-1)^{i-1} \binom{q}{2i} (Ca^2)^i D^{\frac12(q-1)-i} , \tag{13}$$

b given in lemma 1. Putting $a = 3^s a_1$, $(a_1,3) = 1$, $s \geqq 1$ we observe that the first teım on the right-hand side of (13) is exactly divisible by $3^{\delta+2s+\mu}$, where $\mu = 1$ or 0, according as $C \equiv 0 \pmod 3$ or not, and $q-1 = 2q_1 \cdot 3^\delta$, $(q_1,3) = 1$, $\delta \geqq 0$. The general term in the sum in (13) may be written in the form

$$\binom{q}{2} a^2 \binom{q-2}{2i-2} \frac{a^{2i-2}}{i(2i-1)} D^{\frac12(q-1)-i} C^i .$$

Here we have $3^{2i-2} > i(2i-1)$ for $i \geqq 2$, and consequently, this term is divisible by a power of 3 with exponent greater than $\partial + 2s + \mu$. Hence the right-hand side of (13) is exactly divisible by $3^{\delta+2s+\mu}$. In case $q \equiv 1 \pmod 4$ the left-hand side of (13) can be written $D^{\frac12(q-1)} - (-1)^{\frac14(q-1)} 2^{\frac12(q-1)}$, and it is easily seen that $aC \equiv 0 \pmod 3$ implies $q \equiv 1 \pmod 8$. Putting further $D^2-4 = 3^m D'$, $(D',3) = 1$, $m \geqq 1$, we find that the quantity on the left-hand side of (13) is exactly divisible by $3^{\delta+m}$. Hence $m = 2s+\mu$, and our lemma is proved for $q \equiv 1 \pmod 4$. In case $q \equiv 3 \pmod 4$ the left-hand side of (13) may be written

$$(D+2b)\frac{D^{\frac12(q-1)}+(2b)^{\frac12(q-1)}}{D+2b},$$

where the second factor is exactly divisible by 3^δ and therefore $D+2b$ exactly divisible by $3^{2s+\mu}$. This completes the proof of lemma 2.

Lemma 3. *The equation* (4) *is impossible in integers x,y with* $q \equiv 3 \pmod 4$ *if*

$$a^2 \equiv 1 \pmod 3,$$
$$C \equiv D \equiv \varepsilon \pmod 4, \qquad C \equiv D \equiv \varepsilon_1 \pmod 3,$$
$$CD \equiv 3+2\varepsilon\varepsilon_1 \pmod 8,$$

where $\varepsilon = \pm 1$, $\varepsilon_1 = \pm 1$.

Proof. From (4) it follows, $q \equiv 3 \pmod 4$

(14)
$$b \cdot 2^{\frac12(q-1)} \equiv D^{\frac12(q-1)} \sum_{j=0}^{\frac12(q-1)} \binom{q}{2j+1}(-1)^j \equiv \varepsilon_1 \sum_{j=0}^{\frac12(q-1)} \binom{q}{2j+1}(-1)^j \pmod 3.$$

Expanding $(1+i)^q$, $i=(-1)^{\frac12}$, by the binomial theorem it is easily shown that the sum in (14) has the value $(-1)^{\frac14(q-3)}\,2^{\frac12(q-1)}$. Hence,

$$b \equiv \varepsilon_1(-1)^{\frac14(q-3)} \pmod 3.$$

By means of lemma 1 this congruence can be written

$$(-1)^{\frac12(1+\varepsilon\varepsilon_1)} \equiv \varepsilon\varepsilon_1 \pmod 3,$$

which is clearly impossible.

Lemma 4. *A necessary condition that equation* (4) *be satisfied with*

$$a^2 \equiv 1 \pmod 3, \qquad C \equiv D \equiv \varepsilon \pmod 4, \qquad C \equiv -D \equiv \varepsilon_1 \pmod 3,$$

where $\varepsilon = \pm 1$, $\varepsilon_1 = \pm 1$, *is that, either*

$$q \equiv 1 \pmod 8 \quad \textit{or} \quad q \equiv 2(1-\varepsilon\varepsilon_1) - CD \pmod 8.$$

Proof. From (4) it now follows that

$$b\,2^{\frac12(q-1)} \equiv C^{\frac12(q-1)} \sum_{j=0}^{\frac12(q-1)} \binom{q}{2j+1} \equiv C^{\frac12(q-1)}\,2^{q-1} \pmod 3.$$

Hence

(15)
$$b \equiv (2C)^{\frac12(q-1)} \equiv D^{\frac12(q-1)} \pmod 3.$$

In case $q \equiv 1 \pmod 4$ we get

$$(-1)^{\frac{1}{4}(q-1)} \equiv 1 \pmod{3}, \quad \text{that is,} \quad q \equiv 1 \pmod{8}\,.$$

When $q \equiv 3 \pmod{4}$, we can write (15) in the following form:

$$(-1)^{\frac{1}{4}(q+CD)} \equiv \varepsilon\varepsilon_1 \pmod{3}$$

or

$$(-1)^{\frac{1}{4}(q+CD)} \equiv (-1)^{\frac{1}{2}(1-\varepsilon\varepsilon_1)} \pmod{3}\,,$$

that is,

$$\tfrac{1}{4}(q+CD) \equiv \tfrac{1}{2}(1-\varepsilon\varepsilon_1) \pmod{2}\,.$$

Our lemma is proved.

Lemma 5. *The equation* (4) *is impossible in integers x,y with $q \equiv 3$* (mod 4) *if*

$$C \equiv D \equiv \varepsilon \pmod{4}\,,$$

$$C \equiv \varepsilon_2 D \equiv \varepsilon_1 \pmod{5}\,,$$

$$CD \not\equiv 1+2(1-\varepsilon\varepsilon_1\varepsilon_2) \pmod{8}, \qquad \varepsilon = \pm 1,\ \varepsilon_i = \pm 1\,,$$

$i = 1,2.$

Proof. If $a^2 \equiv \varepsilon_2 \pmod{5}$ it follows from (4), using that $q \equiv 3 \pmod{4}$,

$$b\,2^{\frac{1}{2}(q-1)} \equiv (C\varepsilon_2)^{\frac{1}{2}(q-1)} \left(\binom{q}{1} - \binom{q}{3} + \binom{q}{5} - + \ldots\right)$$

$$\equiv (C\varepsilon_2)^{\frac{1}{2}(q-1)}\, 2^{\frac{1}{2}(q-1)}\, (-1)^{\frac{1}{4}(q-3)} \pmod{5}\,.$$

This congruence can be written

$$b \equiv C\varepsilon_2(-1)^{\frac{1}{4}(q-3)} \pmod{5}$$

or

$$-\varepsilon(-1)^{\frac{1}{4}(q+CD)} \equiv \varepsilon_1\varepsilon_2(-1)^{\frac{1}{4}(q-3)} \pmod{5}$$

or

$$(-1)^{\frac{1}{4}(CD-1)} \equiv \varepsilon\,\varepsilon_1\,\varepsilon_2 \pmod{5}\,,$$

which implies $CD \equiv 1+2(1-\varepsilon\varepsilon_1\varepsilon_2) \pmod{8}$, a contradiction. If $a^2 \equiv -\varepsilon_2$ (mod 5) we conclude that

$$b\,2^{\frac{1}{2}(q-1)} \equiv (-C\varepsilon_2)^{\frac{1}{2}(q-1)} \left(\binom{q}{1} + \binom{q}{3} + \binom{q}{5} + \ldots\right)$$

$$\equiv (-C\varepsilon_2)^{\frac{1}{2}(q-1)}\, 2^{q-1} \pmod{5}\,.$$

Hence

$$b \equiv (-C\varepsilon_2)^{\frac{1}{2}(q-1)}\, 2^{\frac{1}{2}(q-1)} \not\equiv \pm 1 \pmod{5}\,,$$

because $2^{\frac{1}{2}(q-1)} \not\equiv \pm 1 \pmod{5}$ in case $q \equiv 3 \pmod{4}$.

It is impossible that $a \equiv 0 \pmod{5}$. This follows from (13) since $D \pm 2 \not\equiv 0 \pmod{5}$.

Our lemma is proved.

Lemma 6. *The equation* (4) *is impossible in integers* x,y *with* $q \equiv 3 \pmod 4$ *if*

$$C \equiv D \equiv \varepsilon \pmod 4 ,$$
$$C \equiv 2\varepsilon_2 D \equiv \varepsilon_1 \pmod 5 ,$$
$$D + 2\varepsilon_1\varepsilon_2 = 5^{2m+1}D', \quad (D',5) = 1 ,$$
$$q \not\equiv 2(1-\varepsilon\varepsilon_1\varepsilon_2) - CD \pmod 8, \ \varepsilon = \pm 1 ,$$

and $\varepsilon_i = \pm 1$, $i = 1,2$.

Proof. At first we need a proof of the following two formulas

$$\sum_{j=0}^{\frac{1}{2}(q-1)} \binom{q}{2j+1} 2^j \equiv (-1)^{\frac{1}{6}(q-\nu)} \pmod 5 ,$$
$$\sum_{j=0}^{\frac{1}{2}(q-1)} (-1)^j \binom{q}{2j+1} 2^j \equiv (-2)^{\frac{1}{6}(q+3-4\nu)} \pmod 5 ,$$

where $q \equiv \nu \pmod 6$, $\nu = \pm 1$. The first one is easily deduced, expanding $(1+(2)^{\frac{1}{2}})^q$ by the binomial formula, and observing that $(1+(2)^{\frac{1}{2}})^6 \equiv -1 \pmod 5$. The second formula can be obtained in the same way, using $1+i(2)^{\frac{1}{2}}$ instead of $1+(2)^{\frac{1}{2}}$ and the fact that $(1+i(2)^{\frac{1}{2}})^6 \equiv -2 \pmod 5$.

If $a^2 \equiv \varepsilon_2 \pmod 5$ it follows from (4), $q \equiv 3 \pmod 4$

$$\begin{aligned} b\,2^{\frac{1}{2}(q-1)} &\equiv (C\varepsilon_2)^{\frac{1}{2}(q-1)} \left(\binom{q}{1} + 2\binom{q}{3} + 4\binom{q}{5} + \dots \right) \\ &\equiv C\varepsilon_2(-1)^{\frac{1}{6}(q-\nu)} \pmod 5 . \end{aligned}$$

However, this is impossible, since $2^{\frac{1}{2}(q-1)} \not\equiv \pm 1 \pmod 5$.

If $a^2 \equiv -\varepsilon_2 \pmod 5$ we obtain from (4), $q \equiv 3 \pmod 4$

$$\begin{aligned} b\,2^{\frac{1}{2}(q-1)} &\equiv (-C\varepsilon_2)^{\frac{1}{2}(q-1)} \left(\binom{q}{1} - 2\binom{q}{3} + 4\binom{q}{5} - + \dots \right) \\ &\equiv (-C\varepsilon_2)(-2)^{\frac{1}{6}(q-4\nu+3)} \pmod 5 . \end{aligned} \tag{16}$$

Since $q \equiv 4 + 2(1-\varepsilon\varepsilon_1\varepsilon_2) - CD \pmod 8$, we have

$$\tfrac{1}{4}(CD+q) \equiv 1 + \tfrac{1}{2}(1-\varepsilon\varepsilon_1\varepsilon_2) \pmod 2 ,$$

that is,

$$b = \varepsilon(-1)^{\frac{1}{2}(1-\varepsilon\varepsilon_1\varepsilon_2)} = \varepsilon_1\varepsilon_2 . \tag{17}$$

Inserting this in (16) we obtain

$$\varepsilon_1\varepsilon_2 2^{\frac{1}{2}(q-1)} \equiv -\varepsilon_1\varepsilon_2(-2)^{\frac{1}{6}(q-4\nu+3)} \pmod 5 .$$

Since $\frac{1}{2}(q-1) - \frac{1}{6}(q-4\nu+3) \equiv 2 \pmod 4$ and $2^4 \equiv 1 \pmod 5$ we conclude $2^2 \equiv 1 \pmod 5$, which is impossible.

A necessary condition that (4) be satisfied in integers x,y with $q\equiv 3 \pmod 4$ and $a \equiv 0 \pmod 5$ is $D+2b = 5^{2m_3}D'$, $(5,D')=1$. This is easily verified applying the same method as in the proof of lemma 2, replacing the prime 3 by 5. Now, b is given by (17), and our lemma is proved.

2. Proof of a basic formula.

In this section we prove the following formula:

$$F_n(x) = \frac{x^n-1}{x-1} - (-1)^{\frac{1}{8}(n^2-1)}\left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{n-1} \tag{18}$$

$$= \sum_{k=1}^{\frac{1}{2}(n-1)} A_k \left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{n-2k-1}\left(\frac{x^2+1}{2}\right)^k, \quad n \text{ odd}\,,$$

where the coefficients A_k are rational integers. The two first coefficents are

$$n \equiv 1 \pmod 4, \quad A_1 = 0 \quad \text{and} \quad A_2 = (-1)^{\frac{1}{4}(n+3)}\tfrac{1}{4}n(n-1)\,,$$
$$n \equiv 3 \pmod 4, \quad A_1 = (-1)^{\frac{1}{4}(n-3)}n \quad \text{and} \quad A_2 = (-1)^{\frac{1}{4}(n+1)}\tfrac{1}{4}n(n-3)\,.$$

Proof. In (9) we put $y=1$ and $m=n$, then getting

$$\frac{x^n-1}{x-1} = \sum_{r=0}^{\frac{1}{2}(n-1)} \frac{n}{n-r}\binom{n-r}{r}\left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{n-2r-1} 2^{\frac{1}{2}(n-1)-r}\, x^r\,. \tag{19}$$

Since

$$x = \frac{x^2+1}{2} - \left(\frac{x-1}{2^{\frac{1}{2}}}\right)^2$$

we rewrite (19) in the form

$$\frac{x^n-1}{x-1} = \sum_{r=0}^{\frac{1}{2}(n-1)} \frac{n}{n-r}\binom{n-r}{r}\left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{n-2r-1}\cdot$$

$$\cdot \sum_{k=0}^{r}(-1)^{r-k}\binom{r}{k}\left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{2r-2k}\left(\frac{x^2+1}{2}\right)^k 2^{\frac{1}{2}(n-1)-r}$$

or

$$\frac{x^n-1}{x-1} = \sum_{k=0}^{\frac{1}{2}(n-1)} A_k \left(\frac{x-1}{2^{\frac{1}{2}}}\right)^{n-2k-1}\left(\frac{x^2+1}{2}\right)^k, \tag{20}$$

where

$$A_k = \sum_{r=k}^{\frac{1}{2}(n-1)} \frac{n}{n-r}\binom{n-r}{r} 2^{\frac{1}{2}(n-1)-r}\,(-1)^{r-k}\binom{r}{k}\,. \tag{21}$$

Putting $x=i$ in (20) and using the fact that $(i-1)/2^{\frac{1}{2}}$ is a primitive eighth root of unity, it is easily found that

$$A_0 = \sum_{r=0}^{\frac12(n-1)} \frac{n}{n-r}\binom{n-r}{r} 2^{\frac12(n-1)-r}(-1)^r = (-1)^{\frac18(n^2-1)}.$$

Differentiating both sides of (20) with respect to x, then putting $x=i$ we find the values of A_1. Repeating this operation we obtain the values of A_2, and our formula (18) is proved.

In proving theorem 1 we shall make use of formula (18). However, it is necessary to establish a lemma concerning the coefficients A_k, $k>2$, by reason of the quite complicated expression (21).

Lemma 7. *Let d denote any positive integer and put $n-1=2^\delta\cdot n_1$, $(n_1,2)=1$, $\delta \geqq 2$. In the sequence $\{A_k 2^{dk}\}$, $k=2,3,4,\dots$, the first term is exactly divisible by $2^{\delta-2+2d}$, while the following ones are divisible by a power of 2 with exponent greater than $\partial-2+2d$.*

Proof. In the expression (21) for A_k we put $r+s=\frac12(n-1)$, and summing with respect to s, we find

$$A_k = \sum_{s=0}^{\frac12(n-1)-k} \frac{n}{\frac12(n+1)+s}\binom{\frac12(n+1)+s}{\frac12(n-1)-s}(-1)^{\frac12(n-1)-s-k}\, 2^s \binom{\frac12(n-1)-s}{k},$$

or

$$(22)\quad A_k = \tfrac12 n(n-1)\binom{\frac12(n-3)}{k-1}\frac{(-1)^{\frac12(n-1)-k}}{k} +$$

$$+\sum_{s=1}^{\frac12(n-1)-k} \tfrac12 n(n-1)\binom{\frac12(n-1)+s}{s}\frac{(k+s-1)!\,(-1)^{\frac12(n-1)-s-k}}{k!\,1\cdot3\cdot5\cdot\ldots\cdot(2s+1)},\quad k\geqq 1.$$

Obviously each term in the sum ($s\geqq 1$) is divisible by $2^{\delta-1}$. If k is an *odd* number, then it easily follows that $A_k 2^{kd}$ is at least divisible by $2^{\delta-1+dk}$. The term $A_2 2^{2d}$ is exactly divisible by $2^{\delta-2+2d}$. In case $k>2$ and *even*, then $A_k 2^{kd}$ is at least divisible by 2^N, where

$$N \geqq \delta-1-\tfrac12 k+dk \geqq \delta-3+4d > \delta-2+2d,$$

because $k^{-1}2^{\frac12 k}\geqq 1$ for $k\geqq 4$. The lemma is proved.

3. Proof of theorem 1.

Putting $x=\lambda/\lambda'$, where

$$\lambda = \frac{aC^{\frac12}+(-D)^{\frac12}}{2^{\frac12}} \quad\text{and}\quad \lambda' = \frac{aC^{\frac12}-(-D)^{\frac12}}{2^{\frac12}},$$

we get from (18), when $n=q$

$$(23)\quad \frac{\lambda^q-\lambda'^q}{\lambda-\lambda'} - (-1)^{\frac{1}{8}(q^2-1)}\left(\frac{\lambda-\lambda'}{2^{\frac{1}{2}}}\right)^{q-1} = \sum_{k=1}^{\frac{1}{2}(q-1)} A_k \left(\frac{\lambda-\lambda'}{2^{\frac{1}{2}}}\right)^{q-2k-1}\left(\frac{\lambda^2+\lambda'^2}{2}\right)^k .$$

The equation (4) implies

$$(24)\qquad \frac{\lambda^q-\lambda'^q}{\lambda-\lambda'} = b\,.$$

We distinguish between two cases:

1° $q\equiv 1 \pmod 4$. According to lemma 1 we have $b=(-1)^{\frac{1}{4}(q-1)}$. Using (24) we then obtain from (23), remembering that $A_1=0$

$$(25)\qquad (-1)^{\frac{1}{4}(q+3)}(D^{\frac{1}{2}(q-1)}-1) = \sum_{k=2}^{\frac{1}{2}(q-1)} A_k(-D)^{\frac{1}{2}(q-1)-k}\left(\tfrac{1}{2}(Ca^2-D)\right)^k .$$

2° $q\equiv 3 \pmod 4$. According to lemma 1 we have $b=-\varepsilon(-1)^{\frac{1}{4}(CD+q)}$. From (23) we now obtain

$$(26)\quad (-1)^{\frac{1}{4}(q+1)}\left(D^{\frac{1}{2}(q-1)}+\varepsilon(-1)^{\frac{1}{4}(CD+3)}\right) = \sum_{k=1}^{\frac{1}{2}(q-1)} A_k(-D)^{\frac{1}{2}(q-1)-k}\left(\tfrac{1}{2}(Ca^2-D)\right)^k .$$

Our starting point is the equation (25). Putting $\frac{1}{2}(Ca^2-D)=2^dA$, $(A,2)=1$, $d\geqq 1$, we find, using lemma 7 with $n=q$, $\partial\geqq 2$, that the right-hand side of (25) is exactly divisible by $2^{\delta-2+2d}$, while the left-hand side, written in the form

$$(27)\qquad (-1)^{\frac{1}{4}(q+3)}(D^2-1)\,\frac{D^{2^{\delta-1}q_1}-1}{D^{2^{\delta-1}}-1}\;\frac{D^{2^{\delta-1}}-1}{D^2-1}$$

is easily seen to be divisible exactly by $2^{\delta-2+2m+1}=2^{\delta-1+2m}$, that is, $2m+1=2d$, a contradiction.

As to the second part of the theorem, where $D^2-1=2^{2m_1}D_1$, $(D_1,2)=1$, and consequently $m_1\geqq 2$, we note that the second factor in the product (27) is congruent to $q_1 \pmod 8$, while the third factor can be written $2^{\delta-2}(8T+1)$, since

$$D^{2t}+1 \equiv 2 \pmod{16} \quad\text{for}\quad t=1,2,3,\ldots .$$

Dividing both sides of the equation (25) by 2^{-2+2d}, we obtain

$$(-1)^{\frac{1}{4}(q+3)}D_1q_1 \equiv (-1)^{\frac{1}{4}(q+3)}\,qq_1 \pmod 8\,,$$

or

$$q \equiv D_1 \pmod 8\,.$$

Here we have used lemma 7, noticing that

$$\delta-3+4d \geqq \delta-1+3d$$

and

$$(\delta-1+3d)-(\delta-2+2d) \geqq 3 \quad\text{for}\quad d=m_1\geqq 2\,.$$

Our theorem is proved.

4. Proof of theorem 2.

The following formulas are easily verified

$$\left(\frac{\lambda^{\frac{1}{2}(q+1)}-\lambda'^{\frac{1}{2}(q+1)}}{\lambda-\lambda'}\right)^2-\lambda\lambda'\left(\frac{\lambda^{\frac{1}{2}(q-1)}-\lambda'^{\frac{1}{2}(q-1)}}{\lambda-\lambda'}\right)^2=\frac{\lambda^q-\lambda'^q}{\lambda-\lambda'}, \tag{28}$$

$$\frac{\lambda^{\frac{1}{2}(q+1)}-\lambda'^{\frac{1}{2}(q+1)}}{\lambda-\lambda'}\left(\lambda^{\frac{1}{2}(q-1)}+\lambda'^{\frac{1}{2}(q-1)}\right)=\frac{\lambda^q-\lambda'^q}{\lambda-\lambda'}+(\lambda\lambda')^{\frac{1}{2}(q-1)}. \tag{29}$$

$$\frac{\lambda^{\frac{1}{2}(q-1)}-\lambda'^{\frac{1}{2}(q-1)}}{\lambda-\lambda'}\left(\lambda^{\frac{1}{2}(q+1)}+\lambda'^{\frac{1}{2}(q+1)}\right)=\frac{\lambda^q-\lambda'^q}{\lambda-\lambda'}-(\lambda\lambda')^{\frac{1}{2}(q-1)}. \tag{30}$$

1° $q=8t+5$. By means of (28) we get

$$\left(\frac{\lambda^{4t+3}-\lambda'^{4t+3}}{\lambda-\lambda'}\right)^2-\lambda\lambda'\left(\frac{\lambda^{4t+2}-\lambda'^{4t+2}}{\lambda^2-\lambda'^2}\right)^2(\lambda+\lambda')^2=b=-1. \tag{31}$$

This implies

$$\lambda\lambda'(\lambda+\lambda')^2=(Ca^2+D)Ca^2\equiv 1+CD\equiv 2 \pmod 8,$$

that is

$$CD\equiv 1 \pmod 8. \tag{32}$$

From (31) we also conclude that $C\equiv 3 \pmod 4$ is impossible, since -1 is not a quadratic residue modulo a prime of the form $4k+3$. Making use of (30) we obtain

$$\frac{\lambda^{4t+2}-\lambda'^{4t+2}}{\lambda^2-\lambda'^2}\,\frac{\lambda^{4t+3}+\lambda'^{4t+3}}{\lambda+\lambda'}\,2Ca^2=-\left(1+(\lambda\lambda')^{4t+2}\right). \tag{33}$$

Since q is a prime we have $t\not\equiv 2 \pmod 3$. If $t\equiv 0$ or $1 \pmod 3$ we observe that

$$\frac{\lambda^3+\lambda'^3}{\lambda+\lambda'}=\tfrac{1}{2}(Ca^2-3D)$$

is a divisor of the left-hand side of (33). Let p be an odd prime dividing $\frac{1}{2}(Ca^2-3D)$; then p divides $1+(\lambda\lambda')^{4t+2}$, that is, $p\equiv 1 \pmod 4$. Assuming $\frac{1}{2}(Ca^2-3D)>1$, this implies $\frac{1}{2}(Ca^2-3D)=4N+1$ and consequently $CD\equiv 5 \pmod 8$, which contradicts (32). Now $\frac{1}{2}(Ca^2-3D)=+1$ is impossible mod 8, and therefore $\frac{1}{2}(Ca^2-3D)\leqq -1$. Then we have proved:

Necessary conditions for the solubility of (31) *are that*

$$CD\equiv 1 \pmod 8 \quad \textit{and} \quad a^2\leqq (3D-2)/C.$$

2° $q=8t+3$, $q>3$ and $C=1$. We distinguish between two cases.

A. $CD\equiv 1 \pmod 8$. Here is $b=1$, and according to (28)

$$(34) \qquad 2a^2\left(\frac{\lambda^{4t+2}-\lambda'^{4t+2}}{\lambda^2-\lambda'^2}\right)^2 - \lambda\lambda'\left(\frac{\lambda^{4t+1}-\lambda'^{4t+1}}{\lambda-\lambda'}\right)^2 = 1 ,$$

from which it follows that

$$(35) \qquad \lambda\lambda' = \tfrac{1}{2}(a^2+D) \equiv 1 \pmod 8 .$$

By means of (29) we get

$$(36) \qquad 2a^2\frac{\lambda^{4t+2}-\lambda'^{4t+2}}{\lambda^2-\lambda'^2}\,\frac{\lambda^{4t+1}+\lambda'^{4t+1}}{\lambda+\lambda'} = 1+(\lambda\lambda')^{4t+1} .$$

Suppose $a^2 \equiv 1 \pmod 3$. Since $t \equiv 0 \pmod 3$ is excluded, we must have $t \equiv 1$ or $2 \pmod 3$. In both cases

$$\frac{\lambda^3+\lambda'^3}{\lambda+\lambda'} = \tfrac{1}{2}(a^2-3D)$$

is a divisor of the left-hand side of (36). If p is a prime dividing $\frac{1}{2}(a^2-3D)$, we deduce that

$$p > 3, \qquad \left(\frac{3D}{p}\right) = 1 \quad \text{and} \quad \left(\frac{-\frac{1}{2}(a^2+D)}{p}\right) = 1 .$$

This gives $(-2D/p)=1$ and furthermore

$$(37) \qquad \left(\frac{-6}{p}\right) = 1 .$$

The Legendre symbol $(-6/p)$ has the value 1 for the primes $p \equiv 1$, 5, 7 or 11 (mod 24). On account of (35) and the assumption $a^2 \equiv 1 \pmod 3$ we conclude that $\frac{1}{2}(a^2-3D) \equiv -1 \pmod{24}$. If $\frac{1}{2}(a^2-3D) \geqq 1$ this gives a contradiction, and we therefore must have $a^2 \leqq 3D-2$.

Suppose then $a \equiv 0 \pmod 3$. From (34) it follows that $D \equiv 1 \pmod 3$. Putting $a=3a_1$ and observing that $\frac{1}{2}(3a_1{}^2-D) \equiv 13 \pmod{24}$ we obtain, reasoning as above, that the solubility of (36) implies $3a_1{}^2 \leqq D+2$. Using lemma 2 with $(C,3)=1$ it is easily seen that the sign of equality must be excluded. A necessary condition for the solubility of (36) is then $\frac{1}{2}(3a_1{}^2-D) < -1$, or

$$3a_1{}^2 < D-2 \quad \text{where} \quad a = 3a_1 .$$

B. $CD \equiv 5 \pmod 8$. By means of (28) we get, using that $b=-1$

$$(38) \qquad 2a^2\left(\frac{\lambda^{4t+2}-\lambda'^{4t+2}}{\lambda^2-\lambda'^2}\right)^2 - \lambda\lambda'\left(\frac{\lambda^{4t+1}-\lambda'^{4t+1}}{\lambda-\lambda'}\right)^2 = -1 ,$$

from which it follows $\frac{1}{2}(a^2+D) \equiv 3 \pmod 8$. On account of (30) we obtain

$$(a^2-D)\frac{\lambda^{4t+2}+\lambda'^{4t+2}}{\lambda^2+\lambda'^2}\,\frac{\lambda^{4t+1}-\lambda'^{4t+1}}{\lambda-\lambda'} = -\left(1+(\lambda\lambda')^{4t+1}\right).$$

Let p denote an odd prime dividing $\frac{1}{4}(a^2-D)\equiv -1 \pmod 4$ and suppose that $\frac{1}{4}(a^2-D)\geqq 3$. Since p divides $1+(\lambda\lambda')^{4t+1}$ we conclude that

$$\left(\frac{-\frac{1}{2}(a^2+D)}{p}\right) = \left(\frac{-a^2}{p}\right) = 1\,,$$

that is, $p\equiv 1 \pmod 4$, which is impossible. Consequently, $\frac{1}{4}(a^2-D)\leqq -1$, and a necessary condition for the solubility of (38) is that $a^2\leqq D-4$.

Hitherto it is proved that the values of a belong to a finite set, which can be found in a finite number of steps. Now we make use of the result of Cassels mentioned in the introduction. Writing (3) in the form $x^2-(a^2+D)N^2=-D$, where $N=\left(\frac{1}{2}(a^2+D)\right)^{\frac{1}{2}(q-1)}$ it is seen that there are only a finite number of possibilities for the values of q and that these can be determined in a finite number of steps. Then we have proved theorem 2.

5. Proof of theorem 3.

In this section $C=\varepsilon=1$ and $q=8t+7$.

1° $D\equiv 5 \pmod{24}$. The impossibility of (4) and then of (3) is a consequence of lemma 2 in case $a\equiv 0 \pmod 3$ and of lemma 4 when $a^2\equiv 1 \pmod 3$.

2° $D\equiv 13 \pmod{24}$, $D+2=3^{2m+1}D'$, $(D',3)=1$. The theorem follows from lemmas 2 and 3.

3° $D\equiv 9$ or $21 \pmod{40}$. This is an immediate consequence of lemma 5.

4° $D\equiv 15+2\nu \pmod{40}$, $D-2\nu\equiv 5^{2m+1}D'$, $(D',5)=1$, $\nu=\pm 1$. This is proved by means of lemma 6, putting $\varepsilon_2=-\nu\varepsilon_1$.

6. Numerical applications.

It turns out that the following lemma is useful:

LEMMA 8. *A necessary condition that the equation* (4) *be satisfied with* $C=1$, $D\equiv 9 \pmod{24}$ *and* $q\equiv \pm 1 \pmod 8$, *is that* $D\equiv 3 \pmod 9$.

PROOF. From (4) it follows that

$$b\cdot 2^{\frac{1}{2}(q-1)} = (-2)^{\frac{1}{2}(q-1)} = \sum_{i=0}^{\frac{1}{2}(q-1)} \binom{q}{2i+1} (-D)^i\, a^{q-2i-1}\,.$$

This may be written

$$(39)\qquad (-2)^{\frac12(q-1)}-1-q(a^{q-1}-1) = q-1-\binom{q}{3}a^{q-3}D+ \\ +\sum_{i=2}^{\frac12(q-1)}\binom{q}{2i+1}(-D)^i\,a^{q-2i-1}\,.$$

We put $q-1=2\cdot 3^{\delta}\cdot q_1$, $(q_1,3)=1$, $\delta\geqq 1$. Then it is easily shown that $(k^{\frac12(q-1)}-1)/(k-1)$ is divisible by 3^{δ} if $k\equiv 1 \pmod 3$. Using this fact with $k=-2$ and $k=a^2$, we find that the left-hand side of (39) is divisible by $3^{\delta+1}$. Writing the general term in the sum in the right-hand side in (39) in the form

$$\frac{q(q-1)}{2i(2i+1)}\binom{q-2}{2i-2}(-D)^i\,a^{q-2i-1}$$

it is seen that this term is at least divisible by $3^{\delta+1}$, since $3^i/(2i+1)>1$ for $i\geqq 2$. A necessary condition for the solubility of (4) is then that

$$q-1 \equiv \binom{q}{3}a^{q-3}D = \binom{q}{3}a^{q-3}\,3D_1 \pmod{3^{\delta+1}}$$

or

$$2 \equiv (q^2-2q)D_1 \equiv 2D_1 \pmod 3\,,$$

that is, $D_1\equiv 1 \pmod 3$. Our lemma is proved.

We restrict ourselves to the equation $x^2+D=2y^n$.

Example 1. $D=5$, 13, 17 and 21.

According to theorem 1 we must have $q\equiv 3 \pmod 4$. Further it follows from theorem 3 that $q\equiv 7 \pmod 8$ must be excluded. It remains to deal with $q\equiv 3 \pmod 8$, where (section 4,2°)

$$a^2 \leqq D-4 \quad\text{if}\quad D\equiv 5 \pmod 8$$

and

$$a^2 \leqq 3D-2 \quad\text{if}\quad D\equiv 1 \pmod 8\,.$$

The value $a=3$ is impossible. This is obvious if $D=21$ and follows as a consequence of lemma 2 for $D=5$, 13 and 17. If $D=17$, equation (13) also rules out the possibilities $a=5$ and $a=7$. It then only remains the case $a=1$.

In order to determine the possible values of q it is often convenient to tackle the problem by a simple method introduced in [10]. We make use of the following formula [2, p. 748]:

$$(40)\qquad (x+y)^q-x^q-y^q = qxy(x+y)(x^2+xy+y^2)^r\,Q(u,v)\,,$$

where $q>3$ and

$$u = (x^2+xy+y^2)^3,\qquad v = (xy(x+y))^2\,,$$
$$r = 2 \text{ for } q\equiv 1 \pmod 3,\qquad r = 1 \text{ for } q\equiv 2 \pmod 3\,,$$

and $Q(u,v)$ is a polynomial in u and v with integral coefficients. Putting $x=\lambda$, $y=-\lambda'$, we obtain

$$(\lambda-\lambda')^{q-1}-\frac{\lambda^q-\lambda'^q}{\lambda-\lambda'} = -q\lambda\lambda'(\lambda^2-\lambda\lambda'+\lambda'^2)^r\, Q(u,v)\,,$$

or

$$(41)\qquad (-2D)^{\frac{1}{2}(q-1)} \equiv b \pmod{\tfrac{1}{2}(a^2+D)\ \tfrac{1}{2}(a^2-3D)}\,.$$

$D=5$, $a=1$ gives

$$10^{\frac{1}{2}(q-1)} \equiv 1 \pmod{7} \quad\text{or}\quad 2^{q-1}+1 \equiv 0 \pmod{7}\,,$$

which is clearly impossible. In a similar way $D=13$, 17 and 21 can be excluded modulo 7, 3 and 31 respectively. For $q=3$ there is a solution if $D=5$, otherwise not. Then we have proved:

The equation $x^2+D=2y^n$, $n>1$ *and odd, has no solutions in positive integers* x,y *if* $D=13$, 17 *or* 21, *and only one solution given by* $7^2+5=2\cdot 3^3$ *if* $D=5$.

EXAMPLE 2. $D=29$, 53, 61 and 89.

The classnumbers h are 6, 6, 6 and 12 respectively, and we must assume $q>3$. By means of theorems 1 and 3 we conclude that it is only necessary to deal with the case $q\equiv 3 \pmod{8}$. As in the preceding example there are no solutions if $q>3$. In case $D=29$, we find a solution of (4), viz. $117^2+29=2\cdot 19^3$. However, there may be other solutions if $q=3$, such as $5^2+29=2\cdot 3^3$, $1^2+53=2\cdot 3^3$, $25^2+61=2\cdot 7^3$ and $51^2+61=2\cdot 11^3$.

EXAMPLE 3. $D=33$.

By means of theorem 1 and lemma 8 it follows that $q\equiv 3 \pmod{8}$. Since $a\equiv 0 \pmod{3}$ is excluded, we have only to deal with $a=1$, 5 or 7. It turns out that there are no solutions.

EXAMPLE 4. $D=41$ and 73.

These are the only values of $D<100$, where the exponents $q\equiv 1 \pmod{4}$ are not excluded by theorem 1. For $D=41$ we obtain $q\equiv 1 \pmod{8}$ and for $D=73$ we must have $q\equiv 5 \pmod{8}$. $D=73$ is then ruled out by theorem 2. Treating the equation (25) as a congruence mod 25 for $D=41$, it results that (25) is impossible if $q\not\equiv 1 \pmod{5}$. It remains to discuss the case $q\equiv 1 \pmod{40}$. Putting $D=41$ in (39) and observing that $2^{\frac{1}{2}(q-1)}-1\equiv a^{q-1}-1\equiv 0 \pmod{41}$ we get $q\equiv 1 \pmod{41}$. Inserting $q-1=41^{\delta}\cdot 2q_1$, $(41,q_1)=1$, $\delta\geqq 1$ in (39), we obtain that this equation is impossible mod $41^{\delta+1}$. This is easily shown by a reasoning similar to that used in the proof of lemma 8. The case $q\equiv 7 \pmod{8}$ is excluded treating (13) as a congruence mod 7 and using that $41 \equiv -1$ (mod 7) and $73 \equiv -4$ (mod 7). This give the congruences

'42) $$b \cdot 2^{\frac{1}{2}(q+1)} \equiv (a+1)^q-(a-1)^q \pmod 7 \quad \text{for } D = 41$$

and

(43) $$b \cdot 2^{\frac{1}{2}(q+3)} \equiv (a+2)^q-(a-2)^q \pmod 7 \quad \text{for } D = 73\,.$$

Now $a^2 \equiv 1$, $a^2 \equiv 4$ or $a^2 \equiv 9$ (mod 7), since $a \equiv 0$ (mod 7) is excluded by (13). Inserting $a = 1$, 2 and 3 in (42) and (43), it is found that none of these congruences are satisfied. Then we have proved that equation (4) has no solutions in integers x,y if $D = 41$ and $D = 73$.

The only case left is $D = 65$, where theorem 1 shows that $q \equiv 3$ (mod 4). Considering (13) as a congruence mod 11 and using that $65 \equiv -1$ (11) we again get the congruence (42), but now mod 11. After some calculations we find that this congruence is satisfied only if $q \equiv 1$ (mod 5). However, inspecting (13) as a congruence mod 5 we find $q \equiv \pm 2$ (mod 5). Consequently, (13) is impossible in case $D = 65$. Then we have proved:

The equation

$$x^2+D = 2y^n, \qquad n > 3\,,$$

is impossible in integers x and y if $D \equiv 1$ (mod 4) *square-free and* $D < 100$.

REFERENCES

1. J. W. S. Cassels, *On a class of exponential equations*, Ark. Mat. 4 (1963) [No. 17 (1961)], 231–233.
2. L. E. Dickson, *History of the theory of numbers* I. New York, 1952.
3. V. A. Lebesgue, *Sur l'impossibilité d'une équation indéterminée*, Nouv. Ann. Math. (1) 9 (1850), 178–181.
4. D. J. Lewis, *Two classes of diophantine equations*, Pacific J. Math. 11 (1961), 1063–1076.
5. W. Ljunggren, *Über die Gleichungen* $1+Dx^2=2y^n$ *und* $1+Dx^2=4y^n$, Norske Vid. Selsk. Forh. Trondheim 15 (1942), 115–118.
6. W. Ljunggren, *Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen*, Ark. Mat., Astr. Fys. 29 A, No. 13 (1943), 1–11.
7. W. Ljunggren, *On the diophantine equation* $x^2+p^2=y^n$, Norske Vid. Selsk. Forh. Trondheim 16, Nr. 8 (1943), 27–30.
8. W. Ljunggren, *On the diophantine equation* $x^2+D=y^n$, Norske Vid. Selsk. Forh. Trondheim 16, No. 23 (1944), 93–96.
9. W. Ljunggren, *On a diophantine equation*, Norske Vid. Selsk. Forh. Trondheim 18, No. 32 (1945), 125–128.
10. W. Ljunggren, *New theorems concerning the diophantine equation* $Cx^2+D=y^n$, Norske Vid. Selsk. Forh. Trondheim 29, No. 1 (1956), 1–4.
11. W. Ljunggren, *On the diophantine equation* $Cx^2+D=y^n$, Pacific J. Math. 14 (1964), 585–596.

12. T. Nagell, *Des équations indéterminées* $x^2+x+1=y^n$ *et* $x^2+x+1=3y^n$, Norsk Mat. Forenings Skr., Ser. I No. 2, Oslo (1921), 14 pp.
13. T. Nagell, *Sur l'impossibilité de l'équation indéterminée* $z^p+1=y^2$, Norsk Mat. Forenings Skr. Ser. I No. 4 (1921), 10 pp.
14. T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Mat. Forenings Skr. Ser. I No. 13 (1923), 65–82.
15. T. Nagell, *L'analyse indéterminée à degré supérieur*, Mem. Sci. Math. 39, Paris, 1929, 63 pp.
16. T. Nagell, *Sur une équation diophantienne à deux indéterminées*, Norske Vid. Selsk. Forh. Trondheim 7, No. 38 (1935), 136–139.
17. T. Nagell, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. 5 (1954), 153–159.
18. T. Nagell, *On the diophantine equation* $x^2+8D=y^n$, Ark. Mat. 3 (1958) [No. 6 (1955)], 103–112.
19. T. Nagell, *Contributions to the theory of a catogery of diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsal. (4) 16 (1955), 1–38.
20. O. Perron, *Algebra* I, Berlin, 1932.
21. B. Persson, *On a diophantine equation in two unknowns*, Ark. Mat. 1 (1952) [No. 5 (1949)], 45–57.
22. B. Stolt, *Die Anzahl von Lösungen gewisser diophantischer Gleichungen*, Arch. Math. 8 (1957), 393–400.
23. B. Stolt, *Über einen verallgemeinerten Fermatschen Satz*, Acta Arith. 5 (1959), 267–276.
24. C. Störmer, *Solution complète en nombres entiers* m, n, x, y, k *de l'équation* $m \operatorname{arctg}(x^{-1})+n \operatorname{arctg}(y^{-1})=k\frac{1}{4}\pi$, Norske Videnskabsselsk. Skr. Kristiania 1 (1895) No. 11, 21 pp.

UNIVERSITY OF OSLO, NORWAY